WWW.HACKERJOURNAL.IT

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

# HACKER JOURNAL

N° 199

## SICUREZZA: L'ARTE DELLO SNIFFING



## TRAFFICO IN RETE SOTTO CONTROLLO

### MULTI ROUTER TRAFFIC GRAPHER

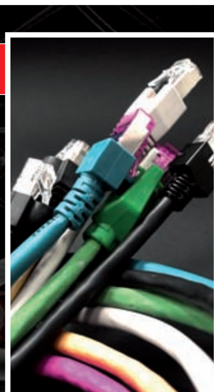
## LOG DI SISTEMA IN MAC OS X

## GOVERNARE LA CENTRALINA DELL'AUTO CON IL TELEFONINO



### MOBILE

›BLOOOVER: ATTACCO AI CELLULARI



### INTERNET

›LA PILA ISO/OSI

### RETI

›OSSEC, SECONDA PARTE

QUATTORD. ANNO 10 - N° 199 - 15 APRILE/28 APRILE 2010 - € 2,00

WLF PUBLISHING

00199
9 771594 577001

EDITORIALE

# UN PERCORSO "TECNICO"

Sono molto contento, davvero, della grande partecipazione, di lettori e iscritti al forum, con idee e progetti per fare crescere la rivista.
E' un piacere scaricare la posta o leggere i vari topic del forum e trovare contributi davvero interessanti. Continuate così.
Ok, finite le "celebrazioni interne", voltiamo pagina.
In questo numero 199, preludio al 200 che attendiamo tutti con grande ansia, si conclude in modo davvero scoppiettante l'articolo su Ossec dell'ottimo Giovanni Federico.
Sono un po' come Mourinho, non mi piace mai parlare molto dei singoli, però questa volta faccio un'eccezione perché questo articolo mi sembra uno dei migliori in assoluto, non parlo solo di HJ, degli ultimi tempi. Davvero godibilissimo. Voi che ne pensate?
Dato a Giovanni quello che è di Giovanni, mi permetto di segnalare, sempre su questo numero 199, anche l'articolo di Rambaldi sulla Pila-ISO, un argomento che viene trattato poco ma che, concettualmente, è molto interessante.
Forse, come qualcuno mi segnala, ci vorrebbe più spazio. Quando articoli come Ossec assorbono da soli 7-8 pagine, non ne rimangono molte per trattare in modo approfondito altri argomenti.
Sarebbe bello avere una rivista da 64 pagine, ma accontentiamoci e godiamo del fatto che si tratta di pagine sempre molto dense, piene, senza pubblicità e, salvo qualche piccolo peccato veniale della redazione, degne di essere lette e conservate con cura.

Un saluto a tutti

Altair

Ps. Ho voluto, rispetto al solito, scrivere questo editoriale in prima persona per manifestare in modo diretto il mio apprezzamento per la partecipazione di tutti, ma si tratta, naturalmente, del pensiero condiviso da parte di tutta la redazione, come sempre. In questo senso siamo molto democratici.

**laboratorio@hackerjournal.it**
**Questo indirizzo è stato creato per inviare articoli, codici, spunti e idee. E' quindi proprio una sorta di "incubatore di idee".**

**posta@hackerjournal.it**
**E' l'account creato per l'omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.**

**redazione@hackerjournal.it**
**Questo è l'indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.**

## Sommario




**Anno 10 - N.199**
**15 aprile / 28 aprile 2010**

**Editore (sede legale)**
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71 - 00196 Roma
Fax 063214606

**Realizzazione editoriale**
Progetti e promozioni Srl
redazione@progettiepromozioni.com

**Printing**
Grafiche Mazzucchelli S.p.a - Seriate (BG)

**Distributore**
M-DIS Distributore SPA
via Cazzaniga 2 - 20123 Milano

**Hacker Journal**
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.
Una copia: 2,00 euro

**Direttore Responsabile**
Teresa Carsaniga
redazione@hackerjournal.it

# NeWS

# LOGICHE E MECCANISMI DI CONSUMO

Ci eravamo ripromessi di non affrontare l'argomento iPad perché tutto sommato se ne parla già tanto e a sproposito, ed è, giustamente o ingiustamente, snobbato a certi livelli (riviste tecniche come questa non dovrebbero forse occuparsene più di tanto…). Tuttavia è una di quelle cose, tipo l'Isola dei Famosi, che nessuno guarda ma di cui tutti, curiosamente, conoscono dettagli, scandali e retroscena. Insomma, per dirla in parole povere, interessa.
Quindi ci sembra interessante analizzare l'argomento dal punto di vista, però, delle linee guida del mercato.
Molti avranno notato una crescita esponenziale nella proposta dei cosiddetti netbook, PC a basso costo equipaggiati con processori non particolarmente potenti e adatti, come suggerisce il nome, per navigare in internet, spedire mail o utilizzare programmi d'ufficio poco esigenti in termini di risorse hardware.
E' un mercato in grandissima crescita ed è logico che Apple lo abbia seguito con grande interesse. Semmai, il problema della casa di Cupertino era, ed è, di non potere realizzare un netbook sotto i 300 dollari perché i margini di guadagno, raffrontati ai costi di produzione, non sono sufficienti.
Quindi Apple è rimasta alla finestra per un po', non potendo collocare portatili sul mercato a quei prezzi.
Non stiamo qui a valutare l'incidenza dei fornitori di Apple rispetto a quelli della concorrenza, quello che ci preme davvero sottolineare è come Apple, in modo geniale, non potendo inserirsi in quel mercato ne abbia creato un altro: quello dei tablet ultraportatili, insomma, dell'iPad.



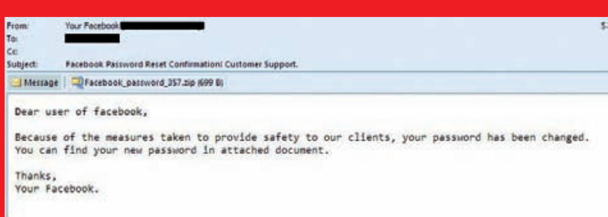

Se ci pensate bene, rispetto alle caratteristiche tecniche l'iPad costa davvero molto, però è bello, stiloso, tutti lo vorranno avere. Design e percezione di grande pregio servono, in buona sostanza, a giustificare un prezzo più alto rispetto a quello dei netbook.
Apple andrebbe studiata da vicino da chiunque voglia approcciare il mercato con qualsiasi prodotto.
Non vende degli apparecchi ma degli ideali. L'iPhone è più caro della maggior parte degli smartphone in circolazione (alcuni dei quali sono decisamente migliori dal punto di vista tecnico) eppure tutti vorrebbero averne uno. Vogliamo poi parlare dell'iPad?
Insomma per sfondare sul mercato l'innovazione e la tecnologia servono solo in parte. Aiutano marketing e idee. Steve Jobs lo sa. E noi?

# NEWS

## CONSUMER THREAT ALERT

Nel suo primo bollettino Consumer Threat Alert, McAfee avvisa i consumatori che il cosiddetto “scareware,” o software antivirus fasullo, potrebbe essere la causa dei principali danni fisici ed economici per gli utenti e i loro computer nel 2010. Grazie al nuovo programma Consumer Threat Alert di McAfee, i consumatori possono ricevere un’allerta immediata sulle minacce on-line più recenti e pericolose con informazioni di intelligence fornite da McAfee Labs direttamente nella casella email.
Per iscriversi al Consumer Threat Alert basta digitare questo indirizzo http://resources.mcafee.com/content/ConsumerThreatAlerts.




# Koobface

## UN WORM ESTREMAMENTE PROLIFICO

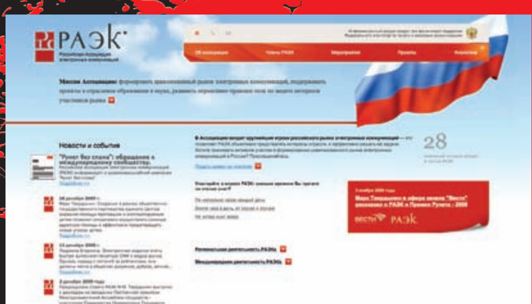
Sono in aumento le infezioni dovute a Koobface, un worm estremamente prolifico capace di infettare i siti di social networking. Questo programma nocivo colpisce siti internet come Facebook o Twitter e riesce a usarli come proxy per i suoi server di comando e controllo. Durante le ultime 2 settimane, il team di ricerca di Kaspersky Lab ha osservato che i server di Comando & Controllo di Koobface sono stati chiusi o ripuliti, con una media di tre volte al giorno. Il numero è costantemente diminuito da 107 (25 febbraio) al livello più basso 71 (8 marzo). In seguito, in sole 48 ore, il numero è cresciuto da 71 a 142, raddoppiando precisamente il numero totale dei server che tutti i computer infettati da Koobface utilizzano per ottenere comandi remoti e aggiornamenti.
Le infrastrutture di comando e controllo Koobface possono essere studiate osservando l’evoluzione della posizione geografica degli indirizzi IP utilizzati per comunicare con i computer infetti. L’utilizzo di server di Comando & Controllo è in aumento soprattutto negli Stati Uniti, con una crescita dal 48% al 52%. Attualmente, più della metà dei server C & C Koobface sono ospitati negli Stati Uniti, percentuali che superano quelle di qualsiasi altro paese nel mondo.

Ecco alcuni suggerimenti agli utenti per difendersi da questo tipo di minacce:

- State attenti ai link nei messaggi sospetti, anche se il mittente è uno dei vostri fidati amici su Facebook.
- Utilizzate un browser aggiornato: Firefox 3.x, Internet Explorer 8, Google Chrome, Opera 10, ecc
- Divulgate il meno possibile informazioni personali. Non date il vostro indirizzo di casa, numero di telefono o altre informazioni private.
- Mantenete il vostro software antivirus aggiornato per evitare che le nuove versioni di malware possano attaccare il computer.

# DALLA RUSSIA CON SPAM

Secondo una ricerca svolta dalla Russian Association of Electronic Communications (RAEC - http://www.raec.ru).
Ai russi spetta la palma di spammer più prolifici. Infatti nella speciale classifica degli spammer sette delle prime dieci posizioni sono occupate da russi, inoltre, il più grande spammer al mondo è proprio un russo.
Vive a Mosca e controlla la più grande rete di vendita di prodotti farmaceutici, attraverso spam, su Internet.
Lo spammer russo ha guadagnato qualcosa come 3,74 miliardi di rubli (127 milioni di dollari) nel 2009. Un quinto di tutte la pubblicità russa Internet è spam.
L'altro aspetto curioso è che USA e Russia, divisi per anni dalla guerra fredda, sembrano collaborare strettamente (quanto inconsapevolmente) a questo genere di attività.
Infatti i server residenti degli USA sono responsabili del 17,3 per cento di tutto lo spam mondiale (che quindi transita attraverso di essi).
Il 16,4 per cento dello spam russo proviene da server residenti negli Stati Uniti. Circa l'83 per cento dei messaggi di spam vengono inviati da "botnet", gli eserciti di computer zombie "reclutati" un po' ovunque all'insaputa degli ignari proprietari.
Infine si rileva come gli annunci relativi a Viagra sono responsabili del 73,7 per cento dello spam in tutto il mondo.







# in Spagna

## I SITI PEER TO PEER NON VIOLANO IL DIRITTO D'AUTORE

Nella delicata materia del Peer to Peer e dei casi di violazione di copyright o altro genere di proprietà intellettuale, ha fatto molto clamore la recente sentenza di un tribunale di Barcellona che ha assolto un sito di peer to peer citato per un presunto reato contro i diritti d'autore.
Il dispositivo della sentenza ha stabilito che offrire link che rimandano ad altri contenuti - anche coperti da copyright, come succede nei P2P - non è illegale.
In senso lato la sentenza riconosce che il "sistema internet" si basa proprio sui link, come accade, ad esempio, per i principali motori di ricerca, quindi chi ospita fa solo da "vettore" non ha responsabilità oggettiva. La responsabilità ricade, semmai, sui siti a cui i link riportano.
Secondo il giudice inoltre le reti P2P, in quanto reti di trasmissione di dati tra privati, non feriscono, in termini generali, alcun diritto protetto dalla legge sulla proprietà intellettuale.
Naturalmente questa sentenza può colmare, a livello giurisprudenziale, solo la normativa spagnola. Qui siamo fermi al decreto Urbani convertito in legge nel 2004. Si tratta di un testo molto controverso che all'epoca aveva suscitato molte resistenze, specie da parte dei Verdi col loro capogruppo Fiorello Cortina..

# :: POSTA ::

## APPROFONDIMENTI SU OPENBSD

Ciao leggo la vostra rivista da ormai più di un anno e la trovo molto interessante in quanto studio da 2 anni informatica da autodidatta (programmazione, reti e sicurezza informatica in generale) e uso linux (Ubuntu 9.10) da parecchi mesi.
Volevo fare i miei complimenti per la rivista piena di informazioni utili e articoli spiegati dettagliatamente.
Interessante l'articolo su OpenBSD lo proverò presto su VMware. Proprio ora sto scaricando l'immagine iso e avevo qualche domanda al riguardo prima di provare il sistema:
1) E' possibile connettersi a reti WEP? Ho letto sull'articolo (forse è un mio errore) che ci si può connettere solo a reti WPA/WPA2, mi sbaglio?
2) E' possibile installare strumenti di analisi/test e studio delle reti quali ad esempio Wireshark, ettercap-ng, nmap o aircrack-ng?
3) A vostro parere è meglio OpenBSD o backtrack 4?

hh

**Andiamo con ordine:**

**1) E' naturalmente possibile connettersi a reti WEP con OpenBSD.**
**Non abbiamo speso molte parole sulla rivista perchè ritiniemo quest'ultimo protocollo decisamente insicuro e "outdated".**
**In ogni caso, riferendoci agli esempi proposti nell'articolo (ipotizzando quindi di voler utilizzare DHCP per l'assegnazione dell'indirizzo), configurare l'if. per l'autenticazione WEP è un gioco da ragazzi; semplicemente andrai ad inserire nel file hostname.interfaccia (nell'articolo: urtw0):**

```
dhcp nwid '<SSID>' nwkey
'<chiave WEP>'
```

**Con ifconfig il discorso non cambia:**

```
ifconfig <INTERFACCIA> nwid
'<SSID>' nwkey '<chiave
WEP>' up
```

**2) Certo, molti di questi li trovi anche precompilati.**
**Ti consiglio inoltre di dare un occhio anche alle bsd-airtools.**
**Trovi il pacchetto per arch. i386 qui: ftp://ftp.spline.de/pub/OpenBSD/4.6/packages/i386/bsd-airtools-0.2p3.tgz**
**Per installarle, come visto nell'articolo, un semplice pkg_add -v bsd-airtools-0.2p3.tgz.**

**3) Non è possibile fare un paragone tra questi 2 sistemi operativi. In primo luogo perchè nascono con target decisamente diversi.**
**Il primo è un OS BSD destinato prevalentemente ad utilizzi server e/o comunque in contesti dove sia richiesta elevata affidabilità e sicurezza.**
**Il secondo è una distro Linux basata su Ubuntu che raccoglie un insieme di applicativi più o meno utili per l'analisi della propria infrastruttura.**
**Tutto quindi dipende da quel che devi fare.**

## GARANZIA SÌ, GARANZIA NO

La risposta data per problemi di garanzia è sbagliata. Per favore correggetela.
La garanzia vale comunque 2 anni senza limitazione alcuna. Nessuna differenza se il guasto è reclamato dopo 1 mese o dopo 23 mesi, lo dice la legge che è al di sopra di eventuali contratti di garanzia che al più dovrebbero aumentare i diritti mai ridurli.
Se HP o altri non vogliono rispetarla basta rivolgersi al Giudice di Pace (anche senza avvocato) scaricate il modulo adatto (se ne trova a volontà) e andate di persona negli uffici del Giudice di Pace. Costa 32 euro circa (grazie alla nuova "tassa" introdotta dal governo Berlusconi da Gennaio 2010). Ripeto non avete bisogno di uno stuolo di avvocati, vedrete che le grandi aziende verranno all' udienza con la soluzione già pronta e se sono molti a seguire questa strada cambieranno subito politica (gli costerà meno).

Giuseppe Grimaldi

**Ringraziamo Giuseppe del contributo. In effetti la normativa europea è piuttosto esplicita nell'indicare i 24 mesi di garanzia, i dubbi, come nel caso del lettore che ha avuto problemi con un computer HP, riguardano il comportamento delle aziende, che spesso cercano di aggirare questa normativa.**
**Comunque l'idea che ci hai suggerito (e che abbiamo tagliato per motivi di spazio) di un articolo che spieghi le modalità per fare ricorso non ci dispiace. La terremo senz'altro in considerazione senza per questo volere portare via il lavoro a "Mi manda Rai Tre".**

# :: POSTA ::

## PROPRIETÀ INTELLETTUALE: DIBATTITO APERTO

Non mi garba la vostra risposta a Giorgio D. nel numero197. Ottima rivista, che seguo assiduamente da anni, senza perdere un numero, però non sempre sono d'accordo. Il mercato esiste perché dà lavoro a persone. Se poi si è bravi programmatori si fanno giochi o programmi che hanno successo, oppure si fanno grandi flop. Un gioco può non valere i 60 euro che ci impongono, ma qualcuno ci ha lavorato e se non li vale è l'utente che spargendone la voce, leggendo i blog, i forum, nei social, ne sancisce il successo. Non credo che la diffusione di Super Mario Bross o Duke, piuttosto di altri giochi simili sia dovuta al caso. Ci sono programmi buoni e meno, ma il rapporto qualità-prezzo ne sancisce il migliore o peggiore giudizio della gente. Se Windows 7 ce lo vendessero a 5 euro ci sarebbe spazio per Linux? Io ho provato tutto: ottimo Firefox, piuttosto che Explorer, più a mio agio con Open Office che con Office, ma Windows ha le sue ragioni se è un passo avanti a Linux. Ho tutti e due su macchine simili e... c'è sempre una ragione. Diamo a Bill quel che è di Bill, che è stato uno dei più grandi geni dei nostri giorni. Io vorrei spezzare una lancia a favore del mercato. Impariamo a pagare la qualità di certi prodotti, a dire no a facili acquisti di prodotti copia cinesi, dalle batterie, ai vestiti fino ai macchinari. Impariamo ad acquistare dove la qualità del prodotto è testata, dove ci sono regole che impongono una leale concorrenza, dove si pagano le tasse, i contributi, le condizioni di lavoro sono garantite, dove chi progetta è premiato e non derubato per la contraffazione. Se poi c'è chi delle sue idee ne vuol far dono, ben venga come benefattore, ma io, dove ne ho la possibilità cerco di acquisire il mio giusto riconoscimento economico, perché non si vive di sola generosità e chi merita va premiato. Bello che la tecnologia possa essere a portata di tutti, ma il mondo ci sta rendendo sempre peggiori e siamo disposti a fare debiti per avere una scomoda Ferrari, piuttosto che comperare con le nostre risorse una comoda monovolume. Accontentiamoci di quello che ci serve e se vogliono farci avere qualcosa in più abbasseranno i prezzi... io non rubo! Io sono orgoglioso di dire che non ho Autocad, anche se a volte per lavoro mi sarebbe utile, e così altri prodotti costosi, ma tutto quello che installo ha regolare licenza!

P.S.

Sarebbe possibile vedere su Journal o Magazine un buon articolo su Wi-Fi e WiMax? Sto cercando di progettare un hot spot privato (se può essere considerato tale) e non ho ancora ben chiaro quali siano gli accessori veramente utili, le distanze copribili in base al guadagno dell'antenna, i permessi necessari, se servono. Grazie e comunque complimentissimi per le riviste.

Enrico P.

**Caro Enrico, sulla prima parte non abbiamo nulla da dire, nel senso che ognuno ha una sua opinione e noi abbiamo pubblicato molto volentieri la tua mail per alimentare il dibattito tra i nostri lettori. Proprietà intellettuale, limiti e sviluppi futuri, questo un po' il tema su cui vorremmo che si sviluppasse la discussione, magari, potrebbe essere interessante aprire un topic sul forum. Per quanto riguarda l'organizzazione di una rete Wi-Fi abbiamo in programma un articolo piuttosto tecnico che potrebbe fare al caso tuo, in cui ci soffermiamo anche ad esaminare la resistenza dei vari materiali al passaggio delle onde Wi-Fi. Segui i prossimi numeri e vedrai che troverai quello fa al caso tuo.**

## IRC

Salve, sono No3X e da molto tempo ormai mi appassiono al pc e in particolar modo al software...
Leggo da anni la vostra rivista e la trovo sempre più interessante in quanto centra esattamente quelli che sono i punti cardine senza dilungarsi in spiegazioni che potrebbero rendere il concetto più complicato.
La vostra rivista è quindi molto completa e ha spiegazioni che abbracciano dai newbie ai veri professionisti.
Tuttavia vi contatto via mail per porgervi una domanda: Sarebbe possibile inserire all'interno della vostra rivista un piccolo inserto su un mondo che magari a volte viene visto come "lamer environment" ma in realtà ha ben più roba... ossia IRC.
Mi spiego meglio.
All'interno di quella che possiamo chiamare rete di IRC esistono aspetti che molte volte restano all'oscuro... e forse a volte vengono sottovalutati. Però vorrei farvi notare come IRC contenga molta roba che potrebbe forse ampliare un po' le comuni conoscenze...
Parlo di Script, Server e poi IRCd, e perché no, quei famosi virus RX che hanno permesso a molte persone di utilizzare il DDoS.
La mia è solo un'idea che porto alla vostra attenzione.

No3X

**Potrebbe essere un'idea, magari la postiamo anche sul forum per capire cosa ne pensano gli altri lettori.**

# :: POSTA ::

## CERTIFICAZIONE COMPLESSA

Ciao ragazzi è la prima volta che vi scrivo e ho l'HJ n.1!!
C'è da dicembre una grossa confusione tra noi professionisti iscritti all'albo. Il ministro ha deciso che le Pa del periodo giurassico devono ricevere le documentazioni tecniche via web, ovviamente contrassegnate con la firma digitale; Il nostro collegio nazionale dei geometri CNG ha stipulato un contratto con Aruba per la PEC e per la così "necessaria" aruba key (letteralmente per lavorare) che si propone come un prodotto innovativo "all in one" fatto a mio parere, apposta per i dinosauri informatici, appunto.
Il CNIPA
http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Firma_digitale/Certificatori_accreditati/Elenco_certificatori_di_firma_digitale/Certificatori_attivi/
E' un ente governativo a sua volta certificante che offre questo tipo di servizi, PEC, firma digitale, smart card e non solo ragazzi! E' anche l'Ente ispettivo di altre aziende certificanti che a loro volta offrono gli stessi servizi per esempio società come l'ACTALIS, infocert,sogei, aruba eccetera.
Adesso faccio due conti:
il CNG (consiglio nazionale dei geometri) fa il contratto con una società, questa società fornirà materiale proprietario? blindato? (Si)
E le pubbliche amministrazioni in fase di ricezione dovranno riconoscere per forza quella impronta "aziendale" di autenticazione o riconosceranno certificati di autenticazione di terze parti presenti nell'elenco di C.A.?
E poi io un lettore (open) con una smart card (open) lo posso comprare sotto casa per pochi euro, mi scarico un programma (open) che implementa la smart, un software (open) che non fa altro che mangiare il file e digerirlo in MIME # p7m, mi autentico ovviamente con la seconda chiave (per firmare il doc.) concertata da contratto con l'azienda che mi ha fornito il servizio, generando "l'ambiente di autenticazione" a monte, et voila. Spedizione via web.
Ma non finisce qui !!! Queste aziende stanno blindando il software che gestisce i driver della smart card chiamandoli "driver certificati".
Addirittura i driver dei lettori stessi.
Quindi se il collegio mi vincola mi incazzo! alla faccia della libertà...
D'altronde il catasto AgdT ha fatto così, per trasmettere gli accatastamenti, per esempio, mi è stato rilasciato regolare certificato di firma digitale, questo mi permette di lavorare ovunque mi trovo (MA SOLO CON LORO), NON con altre Pa, ma come? Dal software "firma e verifica" se entri in gestione certificati vedi che non solo puoi dialogare/loggarti con l'AgdT/sister, ma anche con le dogane e l'agenzia delle entrate!!!
Non mi ha detto niente nessuno.
Nemmeno il manuale, e nel contratto, anzi qualcuno ha detto "...non lo fare se no ti revocano tutto, addio accatastamenti".
Che ne dite? E' ora di chiamare la Sogei per dirgli che deve dire al CNIPA che voglio usare la loro autenticazione per mandare via web i documenti anche al comune? o altra Pa?
Ho letto poi secondo la legge (*) che non è consentito utilizzare una coppia di chiavi per funzioni diverse da quelle previste, per ciascuna tipologia, cosa significa?
E' come portarsi 50 carte di identità e codici fiscali dietro?
E la carta di identità elettronica che facciamo?
Non la ficchiamo nel lettore?
L'autenticazione non è unica per tutte le Pa?
Sono sempre io o sono sempre un altro?
Adesso il caos è totale, non fa distinzione, lettore, token, asimmetrica, chiave, firma elettronica/firma digitale, smart card.
I dinosauri si danno fare... fax, posta raccomandata ecc. (sempre legati ad aruba nel caso dei geometri).
Qualcuno più furbetto, un po' spratichito, c'è l'ha fatta via web, ma aspetterà ancora. Forse sono io il furbetto, oppure mi stanno confondendo veramente, credetemi non mi ha dato una risposta coerente nessuno.
Vi prego hacker aiutate gli uomini liberi, quelli che vogliono avere la libertà di scelta.
In bocca al lupo!

Lorenzo D. M.

**E' una mail un po' particolare ma l'abbiamo pubblicata perché offre diversi spunti. Uno in particolare ci interessa, quello della libertà e degli standard digitali. Effettivamente**
**Le soluzioni che spesso vengono adottate non sono le più logiche. A monte, solitamente, c'è una scarsa dose di conoscenza dell'argomento. Ad esempio qualche anno fa Ministero dell'Istruzione, si parla del 19 giugno 2003, ha firmato il un accordo con Sun Microsystems grazie al quale accordo tutte le scuole italiane - oltre 10.700 tra pubbliche e private – avrebbero potuto ottenere gratis il software StarOffice.**
**Ma come? Tutte le pubbliche amministrazioni percorrono la via dell'open source, c'è un'ottima suite, Open Office, totalmente open source e gratuita, e con la scusa di svincolarsi dalle costose licenze di Microsoft si stipula un accordo per un software che non è open source e la cui licenza è saldamente nelle mani di Sun? Dalla padella nella brace...**
**Cradiamo che ci sia spesso molta approssimazione mista a furberia ed è difficile capire dove finisce l'una e inizia l'altra.**
**Ci sono poi dei misteri assoluti. Ad esempio, in ambito musica digitale non si capisce come mai il formato standard sia diventato l'MP3, che è proprietario, ovvero legato a licenza, e non l'ottimo Ogg Vorbis, open source e qualitativamente superiore...**

Massimiliano Rinaldi
redazione@hackerjournal.it

# IL LOG DI SISTEMA IN MAC OSX



**SICUREZZA NEL MAC È TUTTO A POSTO? PER CAPIRLO BASTA ANALIZZARE I LOG DI SISTEMA DELL'AMBIENTE UNIX.**

Un computer Mac OS X effettua diversi log sull'attività in corso nel sistema operativo. Il log di sistema (o registro di sistema) mostra più eventi che coinvolgono la condivisione in qualsiasi modo attraverso la rete, come ad esempio web o server FTP, e la maggior parte delle manifestazioni che comportano modifiche sul sistema operativo. I log sono spesso trascurati e sono consultati solo in caso di un errore del sistema, violazione della protezione, o altro evento catastrofico. Proprio per questo motivo sarebbe molto meglio familiarizzare con le indicazioni riportate dai log di sistema quando le cose vanno bene.
Infatti, se si ha una buona idea di ciò che avviene in circostanze normali, è facile individuare quando le cose che si stanno verificando nel sistema presentano delle anomalie più o meno vistose. I file di log sono semplici file di testo, e ci sono diversi modi per interagire con essi.

## SYSLOG

Syslog è l'evento Logger di sistema scritto originariamente da Eric Allman. Syslog è un componente standard di Unix e altri sistemi Unix.

Invece di fare sì che per ogni applicazione l'autore si debba preoccupare di dove, come, quando debba essere effettuato l'accesso, e di sgravare gli utenti dalla preoccupazione di trovare ogni singolo file di log dei programmi, syslog offre agli sviluppatori una semplice routine di registrazione per accedere ai loro programmi in forma di openlog e altre librerie. Syslog è il demone di registrazione che viene lanciato all'avvio del sistema dal punto di avvio Sistema/ Libreria/StartupItems /SystemLog. Il file /etc/syslog.conf viene letto dal demone syslog come l'avvio, e configura come i processi del demone ricevano e inoltrino i messaggi. Vi è anche un comando chiamato logger che può essere usato interattivamente o da script di shell per creare voci nel registro di sistema (system log).
I programmi che sfruttano syslog per l'accesso, e questo include il kernel Mach, scrivono i loro messaggi a un file speciale, che solo il demone syslog legge. Syslog analizza i messaggi in arrivo in base al suo file di configurazione e realizza una o più di queste quattro azioni:
* Inoltra il messaggio a un demone syslog in esecuzione su un host differenti.
* Aggiunge il messaggio a un file specificato.
* Invia il messaggio a /dev/console.
* Invia il messaggio allo schermo di utenti definiti se sono collegati.

Il file Syslog.conf definisce come i messaggi vengono gestiti in base a due criteri specifici chiamati livelli e strutture. I livelli si riferiscono alla gravità di un evento, e la struttura fa riferimento agli specifici programmi in esecuzione.

## CONFIGURARE SYSLOG PER SEPARARE I MESSAGGI

La directory /var/log è dove la maggior parte dei file di log sono conservati in un sistema Mac OS X.

Syslog è configurato di default per la maggior parte dei messaggi di log nel file /var/log/ system.log. Separati i file di log, vengono creati, per impostazione predefinita per l'autorizzazione di azioni (in genere dati di accesso), messaggi stampante lpr, mail, ftp, e errori NetInfo. Questo è un ragionevole insieme di valori predefiniti. Tuttavia, ai fini della sicurezza del vostro sistema, e a titolo di esempio, è possibile apportare modifiche alla configurazione per isolare i messaggi da sudo e ssh. Tutte le linee nel file /etc/syslog.conf assumono la forma di azione selector <Tab>.
È fondamentale che negli esempi che seguono e, in ogni modifica apportata ai file, che si utilizzi una Tabulazione tra gli oggetti su una linea, o potrebbero verificarsi risultati fortemente indesiderati. Prima di apportare modifiche al file syslog.conf, è bene fare una copia di backup del file originale, per ogni evenienza.
Per il backup del file, aprire il Terminale e digitare il seguente comando:

```
sudo cp / etc / syslog.conf¬
/ etc / syslog.orig.conf.
```

## SEPARARE I MESSAGGI SUDO

Sudo è configurato per i messaggi di log ad un impianto chiamato local2. E così accade che sudo sia il solo programma installato di default in un sistema che utilizza l'impianto local2. Questo rende abbastanza banale la questione di isolare i messaggi generati da sudo. Infatti basta aprire

```
/ etc / syslog.conf n
```

col vostro editor preferito e aggiungere il seguente testo nel file:

```
local2 .*    /var/log/ ¬
sudo.log
```

In questo esempio, abbiamo detto a syslog di selezionare tutti i messaggi dalla struttura local2 a tutti i livelli di gravità e scrivere questi messaggi nel file /var/log/sudo.log.
Syslog non crea un file da solo, così occorre creare il file di log. Inoltre, è possibile impostare correttamente le autorizzazioni per il file e, infine, riavviare syslog per forzarlo a rileggere il suo file di configurazione. Basta aprire il Terminale e digitare i seguenti comandi:

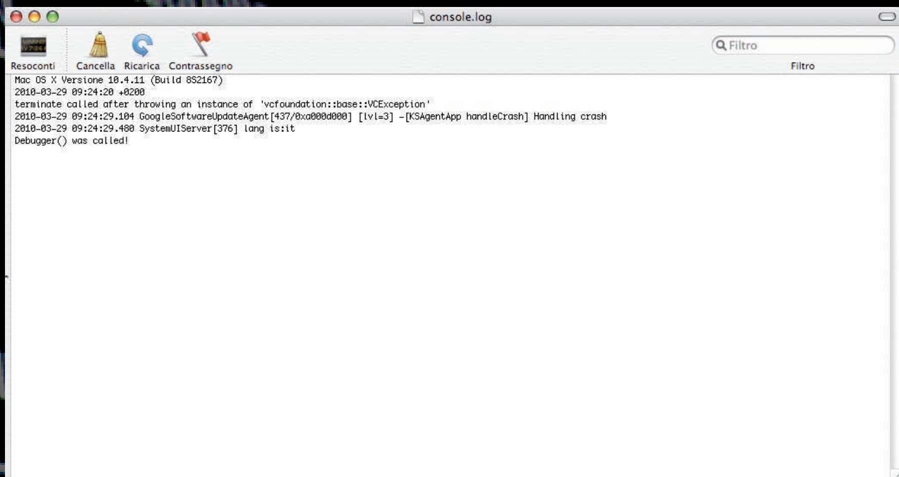
```
sudo touch /var/log/sudo.log
sudo chmod 640 /var/log/¬
sudo.log
sudo kill -HUP `/bin/cat /¬
var/run/syslog.pid`
```

## SEPARARE I MESSAGGI SSH

Se si consente il collegamento al proprio sistema via ssh, è consigliabile accedere a queste connessioni in modo da poterle monitorare. Per fare questo bisogna modificare sia i file di configurazione di sshd e che i file di configurazione di syslog.
Prima aprire il file di configurazione del server SSH che si trova in /etc/ sshd_config con sudo e con il vostro editor preferito e cambiare il valore di SyslogFacility da AUTH a LOCAL7, assicurarsi di aver rimosso il carattere # fin dall'inizio della linea.
Quindi rimuovere il carattere # dalla linea LogLevel immediatamente inferiore. Di seguito salvare il file e chiuderlo.
A questo punto, aprire /etc/syslog.conf nel vostro editor preferito e aggiungere il seguente testo nel file:

```
local7.*        /var/log/¬
sshd.log
```

In questo esempio, si è "ordinato" a syslog di selezionare tutti i messaggi dalla struttura local7 per tutti i livelli di gravità e scrivere questi messaggi nel file /var/log/sshd.log.
Ancora una volta, syslog non può creare file nella directory /var/log per voi, così è possibile creare il file di log con autorizzazioni, quindi riavviare syslog per costringerlo a rileggere il file di configurazione. Per




fare ciò basta aprire il Terminale e digitare il seguente commando:

```
sudo touch /var/log/sshd.log
sudo chmod 640 /var/log/¬
sshd.log
sudo kill -HUP `/bin/cat
/¬var/run/syslog.pid`
```

A questo punto non resta che esaminare i file di log attraverso Terminale o console.
Ora è necessario esaminare questi file per vedere che tipo di eventi si verificano sul computer e assicurarsi che tutto stia andando nel modo che ci si aspetta. Le opzioni sono diverse. È possibile sfogliare i file di log in Terminale o utilizzare la console per visualizzare i messaggi di log. Per il debug di nuovi servizi, e di altri eventi di sistema, esaminare il file di log in tempo reale può essere estremamente utile. Una caratteristica di Leopard (e Snow) è che Apple System Profiler include anche un visualizzatore di file di log. Questo è utile se si ha bisogno di fornire copie dei file di log per i vari tipi di supporto tecnico.

## UTILIZZARE IL TERMINALE PER VISUALIZZARE I FILE LOG

I comandi tail, less, cat, e grep sono molto utili quando si tratta di visualizzazione e di ricerca dei file di log (o file di registro).
Si può utilizzare il comando di tail per vedere la fine di un file di registro digitando tail /var/log/ system.log. Tail può essere utilizzato per monitorare continuamente un file sfruttando l'opzione -f. Tail, quando viene invocato con l'opzione -f, non si ferma quando il marcatore EOF (end-of-file, fine del file) è raggiunto, ma attende un contributo supplementare. A questo punto occorre aprire e guardare un file di log digitando il comando tail-f /var/log/system.log. Quindi sostituire /var/log/ system.log con il file di log precedente.

Si può utilizzare il comando less per scorrere un file di log pagina per pagina. È possibile ricercare all'interno del file che si sta leggendo digitando il carattere / seguito dalla vostra stringa di ricerca (per esempio, /craigz). La prima occorrenza del vostro termine di ricerca verrà evidenziata. È inoltre possibile saltare alla successiva occorrenza digitando N sulla tastiera e continuare a digitare N per spostarsi attraverso gli elementi trovati. È anche possibile spostare, riga per riga, verso il basso, il file utilizzando il tasto Invio o la freccia verso il basso. La freccia verso l'alto può essere utilizzata anche per scorrere verso l'alto riga per riga. Per passare attraverso il documento pagina per pagina, utilizzare la barra spaziatrice.

Se si desidera controllare una specifica stringa di testo nel proprio file di log, è possibile utilizzare il comando cat in combinato disposto con grep. Per esempio, per cercare la stringa craigz nel file di log del sistema, digitare il seguente comando:

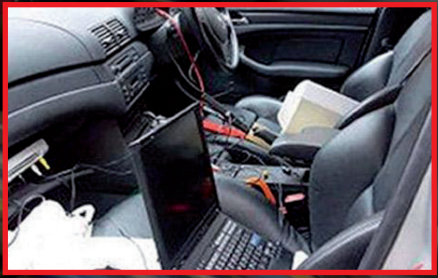
```
cat/var/log/system.log ¬
| grep craigz.
```

## UTILIZZARE CONSOLE PER I FILE DI LOG

L'applicazione console si trova nella cartella Utility all'interno della cartella Applicazioni. Il lato sinistro dell'applicazione visualizza due categorie principali (INTERROGAZIONI DATABASE RESOCONTI e RESOCONTI), all'interno di RESOCONTI trovano spazio i file console.app e system.log, nonché tre cartelle in cui si trovano i log, /Library/Logs, ~ Library/log e /var/log. Ciascuna di queste cartelle ha triangoli che possono essere ciccati per mostrare la visuale estesa ed evidenziare i singoli file di log all'interno.
Una volta che un file viene selezionato a sinistra, il suo contenuto viene mostrato nel lato destro della finestra. La casella di ricerca in alto a destra è classificata come Filtro. È possibile digitare del testo in questa finestra, e solo le linee che contengono la stringa di testo vengono evidenziate nel contenuto finestra. Facendo clic sull'icona di Cancella, viene cancellata la finestra. Utilizzando il pulsante Ricarica si aggiorna la finestra di contenuto, e il pulsante Inserisci Contrassegno inserisce una riga con una serie di trattini per evidenziarla. Il pulsante Inserisci Contrassegno è molto utile se si sta osservando un file per un evento specifico in quanto è possibile inserirlo per marcare la riga e renderla facilmente individuabile.

di Massimiliano Brasile
redazione@hackerjournal.it

# OBDScope



## MONITORING

### Come controllare la centralina del motore direttamente dal proprio telefonino.

Sarà capitato a molti di vedersi accendere una spia sul cruscotto dell'auto per qualche allarme che ci ha subito preoccupato. Obbligatorio, dopo aver letto sul manuale che quella "chiave inglese" indica problemi di elettronica, visitare un'officina autorizzata o un elettrauto, che tramite un computer portatile può collegarsi alla centralina della nostra auto e capire se l'allarme è reale o semplicemente va fatto qualche controllo.
Non vogliamo promuovere con questo articolo il fai-da-te riguardo problemi che possono facilmente impattare con la sicurezza del nostro mezzo, quanto piuttosto cercare di capire quali informazioni possono essere scambiate tra le diverse centraline che ormai sono sparse nell'auto (tra airbag, motore, allarme..). Infatti non sarebbe per lo meno rassicurante sapere subito di che cosa si tratta, collegandoci anche noi al computer di bordo per sapere che errore è stato riscontrato? E in fondo sarebbe anche più divertente, se pensiamo che il tutto si può fare usando proprio il nostro telefonino con Symbian grazie OBDScope, un software che costa 9,95.

## COSA OCCORRE

Oltre al programma, che può essere acquistato online direttamente dal sito dell'autore (obdscope.urli.net) e a un telefonino con Symbian versione 3a o 5a (vedi Box #1), occorre un adattatore bluetooth che possa connettersi alla centralina dell'auto.
Solitamente infatti la centralina è posizionata in posti difficili da raggiungere e viene offerto un connettore in una posizione più facilmente accessibile cui collegare il terminale per la diagnostica.
I connettori dei costruttori di auto sono stati uniformati a livello mondiale nel corso degli anni e si fa genericamente riferimento al protocollo OBD (On-Board Diagnostics). Per l'Europa lo standard di riferimento per le auto prodotte dal 2003 si chiama EOBD (OBD II per Europa). Tipicamente saranno supportati dal programma i modelli a benzina introdotti sul mercato dal 2001 e quelli diesel introdotti dal 2005.




*L'adattatore ELM 327 CAN OBD 2 è tra quelli supportati da OBDScope e si trova online a 89*

***L'elenco dei telefonini supportati ufficialmente da OBDScope è abbastanza ampio, tuttavia se il nostro modello non compare verifichiamo che abbia comunque Symbian ver. 3a o 5a e potremo usarlo comunque.***

Nokia 3250, 5500 Sport, 5700, 6120, 6121, 6290, 6110 Navigator, E51, E60, E61, E61i, E62, E63, E65, E66, E70, E71, E90, N73, N75, N76, N77, N80, N81, N81 8GB, N82, N91, N93, N93i, N95, N95 8GB, E52, E55, E71x, E72, E75, N78, N79, N85, N86 8MP, N96, N97, N97 Mini, 5230, 5320 XpressMusic, 5530 XpressM usic, 5630 XpressMusic, 5730 XpressMusic, 5800 XpressMusic, 6210 Navigator, 6220 Classic, 6650, 6710 Navigator, 6720 Classic, 6730 Classic, 6760 Slide, 6790 Slide, 6790 Surge, X6
Samsung SGH-i400, SGH-i450, SGH-i520, SGH-i550, SGH-i560, SGH-G810, LG KT615 KT610, KS10, i8910
Sony-Ericsson Satio

***Elenco degli adattatori bluetooth OBD-II supportati da OBDScope***

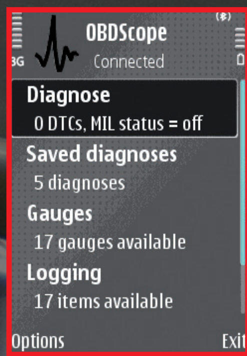
- ELM327 Bluetooth OBD-II Wireless Transceiver Dongle
- OBDKey Bluetooth
- DIAMEX DX70 Bluetooth
- qualunque interfaccia Bluetooth OBD-II che ha a bordo un chip compatibile con ELM

Per quanto riguarda l'adattatore OBD II, OBDScope ne supporta diversi (vedi Box #2) e anch'essi possono essere acquistati online con prezzi a partire da 89 euro. Considerando che un kit portatile di diagnostica professionale ha un prezzo indicativo di 200 euro, è evidente che oltre ad avere una soluzione pratica perché praticamente sempre disponibile si spende praticamente la metà, tra adattatore e software.

## IL PROGRAMMA

OBDScope è gratuito per sette giorni, dopodiché andrà acquistata la regolare licenza. L'installazione è davvero semplice: si scarica dal sito il pacchetto autoinstallante e si lancia il setup.
Supponiamo ora di avere tutto l'occorrente e di aver individuato dove connettere l'adattatore in auto, accendiamo l'interfaccia e assicuriamoci che il telefonino abbia attivo il bluetooth.

Accendiamo il solo quadro comandi dell'auto per alimentare la centralina e lanciamo quindi il software sul telefonino. Da Options selezioniamo Connect e OBDScope tenterà di connettersi alla centralina per avviare lo scambio di informazioni. A questo punto verrà presentato il wizard delle connessioni via bluetooth (a meno che non sia stato memorizzato un precedente "pairing" tra i dispositivi) e una volta concluso il tutto vedremo visualizzato Connected sullo schermo.




***Una volta connesso il software alla centralina viene mostrato l'indicatore Connected e visualizzati a video tutti i dati disponibili nelle diverse schermate.***

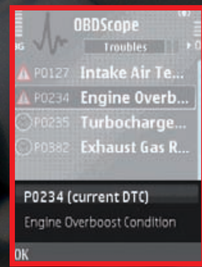
Ora siamo pronti per lanciare le diagnostiche. Apriamo il menu principale e clicchiamo su Diagnose: partirà la raccolta di tutte le informazioni disponibili al programma in base al tipo di veicolo (e di centralina) cui siamo connessi. Una volta terminata questa fase avremo a disposizione quattro finestre per leggere i dati:

Troubles, che raccoglie gli eventuali codici d'errore completi di descrizione che possono essere anche inviati via SMS
FreezeFrame, che permette di visualizzare in dettaglio i dati relativi a un particolare codice d'errore
Diagnosis, che visualizza diverse informazioni di diagnostica che possiamo anche salvare nella memoria del telefonino
OBD Tests, che permette di effettuare un'ampia rosa di test diagnostici (vengono presentati solo i test che possono essere eseguiti).

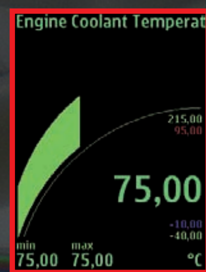
Tramite Gauges (Indicatori), possiamo visualizzare graficamente i dati anche in tempo reale, cioè man mano che vengono elaborati dalla centralina ed analizzare i consumi, le prestazioni e varie informazioni che possono farci capire se il motore funziona correttamente.



***A seconda del modello di auto, può variare la collocazione del connettore OBD; nei modelli recenti è comunque possibile trovarlo all'interno dell'abitacolo.***

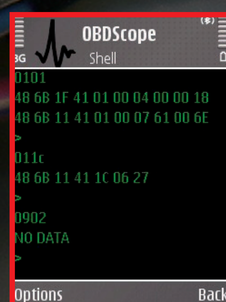



***Quando viene riscontrato un errore, viene mostrata una breve descrizione del messaggio associato.***




***Quando sono disponibili dati di tipo telemetrico, vengono abilitati i grafici in Gauges che permettono di vedere visivamente il comportamento di qualche parametro.***

Una volta raccolte tutte le informazioni, dei vari quadri, possono essere salvate in formato CSV per poterle analizzare su un foglio di calcolo.




***Shell permette di agire davvero a basso livello, ma chiaramente è indicato solo per utenti davvero esperti.***

Tra gli aspetti più interessanti di OBDScope c'è la Shell che permette di inviare comandi di basso livello direttamente in protocollo OBD-II (il che permetterebbe in teoria di abilitare funzionalità disattive ad esempio, che il software non ci rende disponibili) e OBD Trace che permette di osservare tutto il traffico dati scambiato tra il software e la centralina.
Con OBDSCope la nostra auto può finalmente parlarci e dirci come sta.



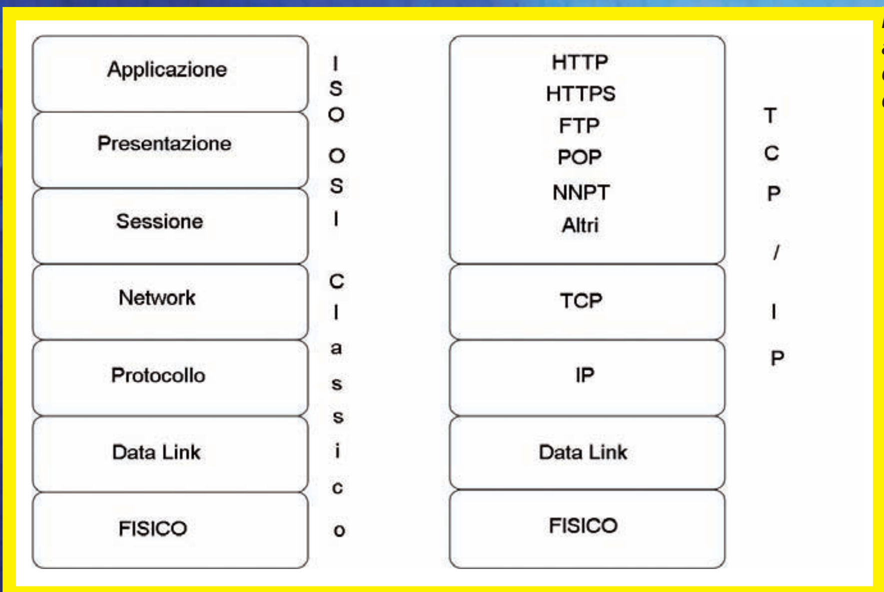


di Raffaele Rambaldi
Raffaele_rambaldi@hotmail.com

# PILA ISO-OSI

INTERNET

## Dietro le quinte della PILA/ISO, responsabile del funzionamento di Internet e non solo...




*In questa figura sono messi a confronto il modello classico della Pila ISO/OSI ed il modello del TCP/IP.*

La pila ISO/OSI è la base del funzionamento delle reti, Internet compreso. Capire il suo funzionamento e perché uno strumento lavora a livello due piuttosto che a livello tre è estremamente importante per capire i meccanismi dei protocolli di rete ed, a cascata, del funzionamento di Firewall e simili. Vediamo come funziona.
Per natura confesso di essere estremamente curioso. Generalmente non mi accontento di conoscere l'effetto di un evento; sono talmente curioso da volerne a tutti i costi conoscere la causa. Per esempio, non mi accontento di sapere che i dati in rete (come in Internet) viaggiano su fibre ottiche, cavi in rame, micro-onde, tam-tam e simili ma voglio sapere anche perché, in che modo e seguendo quali meccanismi. In questo articolo voglio rendervi partecipi di che cosa ho scoperto; ma andiamo con ordine.

### IL MEZZO FISICO

Il mezzo fisico è ovviamente ciò che possiamo toccare: il cavo in rame, la fibra ottica, l'antenna del sistema di trasmissione radio, ossia dei mezzi che vengono utilizzati per trasmettere nell'ordine un segnale elettrico, ottico ed elettromagnetico, per indicare solo i principali.
Questi segnali devono essere organizzati seguendo uno schema preciso che nel caso del cavo in rame può essere la tensione scelta per rappresentare i valori logici, l'ampiezza del segnale ottico (la frequenza luminosa) per le fibre ottiche e la frequenza in Mhz per le onde radio. In comune ci sarà la durata in microsecondi del segnale (clock), oppure la forma ed il sistema di innesto per il collegamento dei connettori tra loro.
E qui si apre un ventaglio estremamente vasto di possibilità che spazia dai connettori coassiali thin e thick Ethernet per arrivare alla categoria 6 per i cavi di rete twistati, alle frequenze infrarosse o ultraviolette delle fibre ottiche che possono a loro volta essere multimodali o monomodali, e la frequenza in Mgz GSM/GPRS/UMTS, WiFi, Bluetooth (banda ISM da 2,45 Ghz a 2,56 Ghz) e chi più ne ha più ne metta.

## DATA LINK

Adesso che abbiamo definito un mezzo trasmissivo occorre che i segnali in transito siano sempre coerenti. A che scopo avere una strada se i segnali che viaggiano al suo interno sono inaffidabili? Allora, sul mezzo fisico dobbiamo costruire un circuito o un meccanismo che sia in grado di gestire il traffico dei dati, fornendo opportuni algoritmi di correzione che intervengano in caso di necessità.
Su questo livello occorre definire una trama (Frame), in grado di trasportare i dati e che abbia un inizio ed una coda che possano essere utilizzati per controllare la coerenza dei dati trasmessi.
Una trama viene trasmessa da una sorgente e ricevuta da un target che deve controllare l'attendibilità di quanto ricevuto per poter a sua volta comunicare alla sorgente che quanto trasmesso è arrivato integro. Esistono molteplici tecnologie come ad esempio Ethernet o ATM, solo per indicarne alcune, ciascuna con svariate sotto-categorie e con la propria implementazione della trama di secondo livello.
Generalmente le trame vengono numerate e la tecnica di controllo si chiama Acknoledge. Essa consiste nell'inviare in risposta alla trama trasmessa una trama in risposta che contenga l'ACK di quanto ricevuto. Questa trama può anche essere cumulativa e contenere l'ACK per diversi pacchetti. Qualora la macchina sorgente non riceva l'ACK per un dato pacchetto in un tempo predeterminato, provvederà a ritrasmetterlo.
Ciascun mezzo trasmissivo rispetta le proprie specifiche di secondo livello. In alcuni casi possono essere implementati meccanismi che regolano anche il traffico ossia la quantità di dati che possono essere trasmessi e ricevuti, provvedendo ad accelerare o rallentare il flusso a seconda delle necessità.
Tra il secondo ed il terzo livello c'è un livello ibrido dove lavorano, ad esempio, le centrali telefoniche a commutazione o gli switch ethernet, in grado di creare delle tabelle di instradamento proprie del livello Network, sfruttando caratteristiche proprie del Data Link.

## NETWORK

Questo livello è il primo di quelli composti da solo software, svincolati dall'hardware che caratterizzava i primi due livelli. La caratteristica principale è quella di stabilire il percorso più efficiente attraverso i diversi mezzi fisici che si trovano a livello più basso. Questo meccanismo si chiama Routing e viene implementato attraverso la creazione di tabelle che indicano i segmenti contigui di indirizzi definiti dalle subnet mask. Il meccanismo è abbastanza semplice e consiste nella definizione di gruppi di indirizzi associando a ciascuno di essi una interfaccia di rete che è in grado di gestire il mezzo fisico utilizzabile per l'instradamento.
Per una centrale telefonica l'equivalente è la creazione del circuito virtuale tra due utenze telefoniche mentre per il protocollo Internet TCP/IP il meccanismo è dato da una entry in una tabella di routing. Essa potrà essere composta da un indirizzo di rete (10.190.0.0), da una subnet (255.255.0.0), da un Gateway (192.168.0.1) e da un parametro metrico che stabilisce la priorità di utilizzo qualora coesistano diversi percorsi per la medesima destinazione.
Infatti, la rete 10.190.0.0 composta da 65.536 indirizzi contigui (256x256), raggiungibile attraverso l'interfaccia 192.168.0.1 può essere raggiunta anche da altre interfacce come ad esempio la 172.64.0.1 e la 10.200.0.1. La scheda di rete Gateway indicata nella tabella di routing con il valore metrico inferiore è quella che avrà la precedenza nella trasmissione del pacchetto.

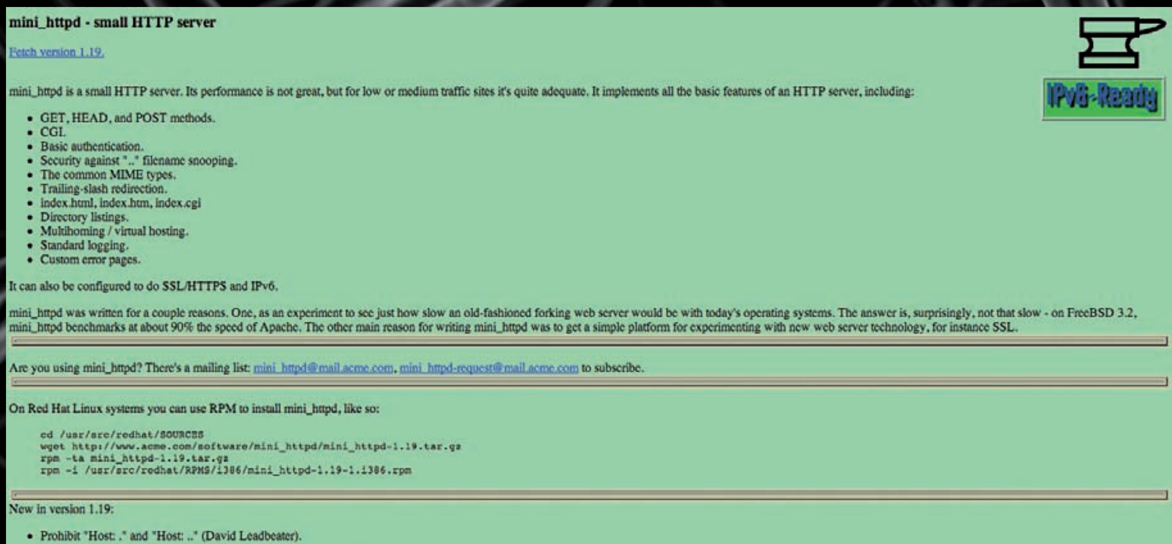
## TRANSPORT

Ormai consideriamo unicamente il TCP/IP e a questo livello si posiziona lo strumento che garantisce alle applicazioni del livello superiore di ricevere e trasmettere un flusso di dati costante. Il Trasporto fa esattamente ciò che viene specificato nel nome, ossia si incarica di gestire a livello logico il punto di arrivo e quello di partenza e non ha idea dei meccanismi di instradamento del livello inferiore e, men che meno, è interessato dalle problematiche connesse al mezzo fisico.
Il flusso di dati ricevuti dall'applicazione che risiede a livello superiore, come vedremo tra un attimo, viene segmentato e trasmesso a pezzetti per poi essere ricostruito ed inviato all'applicazione in attesa sul nodo di destinazione, come se nulla fosse avvenuto.
Magari, nel frattempo i dati hanno attraversato continenti ed oceani, ma per quanto lo riguarda, il Trasporto ha provveduto soltanto a prevenire la congestione, ottimizzando la frequenza di trasmissione dei pacchetti.

## APPLICAZIONE

Il Modello ISO/OSI prevede ulteriori tre strati dove lavorano rispettivamente la sessione, la presentazione e l'applicazione, ma per quanto attiene il TCP/IP, questi tre strati vengono accomunati in uno solo a livello Applicativo.
Nella Sessione operano solamente alcuni protocolli come il NFS (Network File System) utilizzato per accedere a dischi fisici attraverso la rete mentre gli algoritmi di cifratura/decifratura o i protocolli di File Sharing funzionano al livello Presentazione.
Ma quello che veramente ci interessa risiede a livello Applicativo dove troviamo, appunto, le applicazioni che interagiscono con l'utente finale.
Ciascuna di esse è "in ascolto" o "trasmette" su una delle 65.536 porte gestite dal livello Trasporto che scendendo e salendo i vari strati della pila ISO/OSI arriveranno a destinazione.

Massimiliano Rinaldi
redazione@hackerjournal.it



mini_httpd - small HTTP server

Fetch version 1.19.

mini_httpd is a small HTTP server. Its performance is not great, but for low or medium traffic sites it's quite adequate. It implements all the basic features of an HTTP server, including:

- GET, HEAD, and POST methods.
- CGI.
- Basic authentication.
- Security against ".." filename snooping.
- The common MIME types.
- Trailing-slash redirection.
- index.html, index.htm, index.cgi
- Directory listings.
- Multihoming / virtual hosting.
- Standard logging.
- Custom error pages.

It can also be configured to do SSL/HTTPS and IPv6.

mini_httpd was written for a couple reasons. One, as an experiment to see just how slow an old-fashioned forking web server would be with today's operating systems. The answer is, surprisingly, not that slow - on FreeBSD 3.2, mini_httpd benchmarks at about 90% the speed of Apache. The other main reason for writing mini_httpd was to get a simple platform for experimenting with new web server technology, for instance SSL.

Are you using mini_httpd? There's a mailing list: mini_httpd@mail.acme.com, mini_httpd-request@mail.acme.com to subscribe.

On Red Hat Linux systems you can use RPM to install mini_httpd, like so:

```
cd /usr/src/redhat/SOURCES
wget http://www.acme.com/software/mini_httpd/mini_httpd-1.19.tar.gz
rpm -ta mini_httpd-1.19.tar.gz
rpm -i /usr/src/redhat/RPMS/i386/mini_httpd-1.19-1.i386.rpm
```

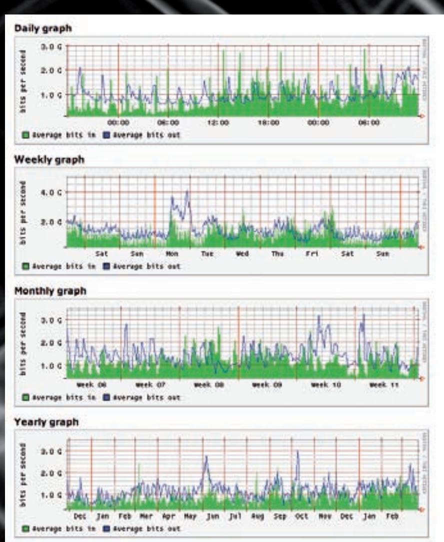
New in version 1.19:

- Prohibit "Host: ." and "Host: .." (David Leadbeater).

# MULTI ROUTER TRAFFIC GRAPHER

MONITORING

## UN OTTIMO STRUMENTO PER MONITORARE IL TRAFFICO IN RETE.




Per tenere sotto controllo una o più macchine remote, il mondo open-source mette a disposizione tantissimo software. Il più semplice da usare e da configurare è, senza ombra di dubbio, MRTG (http://oss.oetiker.ch/mrtg) Iniziamo col dire che sono indispensabili alcune librerie ed alcuni programmi:

```
* [net-analyzer/net-snmp]
* [media-libs/libgd]
* [net-analyzer/mrtg]
* [sys-apps/dcron]
```

Opzionalmente possiamo anche visualizzare remotamente le statistiche avvalendoci di un server web come Mini_httpd <http://www.acme.com/software/mini_httpd/> o Apache <http://www.apache.org>. Vorrei faceste attenzione durante il copia ed incolla dei seguenti comandi. Dato che molti sono sensibili ai cosiddetti “line feed error”, specie quelli che cominciano con:
*/bin/cat -s > /foo/bar* Ricordo inoltre che ad ogni /bin/cat -s, vanno premuti contemporaneamente i tasti: [ctrl] e il tasto [d].

Cominciamo!
Con i permessi di amministratore di sistema (o superutente) creiamo le directory necessarie

```
$su -
Password:       # Digitate la password di amministratore
$mkdir /etc/mrtg
$mkdir /etc/cron.mrtg
$mkdir /var/www/localhost/mrtg
```

Create le directory possiamo cominciare a configurare il nostro file di configurazione snmpd.conf:

```
$/bin/cat -s > /etc/snmp/snmpd.conf
com2sec local      127.0.0.1/32    public
com2sec local      10.10.10.0/24   public

group MyROGroup v1          local
group MyROGroup v2c         local
group MyROGroup usm         local


view all    included  .1        ¬
80
access MyROGroup ""       any         noauth ¬
exact  all    none   none
syslocation MyLocation
syscontact Me
```

Se avete fatto un copia/incolla, ora dovreste premere contemporaneamente i tasti [ctrl]+[d], così da interrompere l'inserimento dei caratteri. Infatti, cat -s, attende un vostro "segnale" prima di procedere con la "concatenazione" finale dell'informazione. Se preferite incollare solo lo script, tralasciatelo :) Questo file consentirà di impostare il servizio snmpd secondo le nostre esigenze, ed evitare di permettere l'accesso in lettura alle persone non addette ai lavori. Ricordo inoltre che snmpd è altamente configurabile, e che un man snmpd risponderà ad ogni vostra ulteriore domanda. Ora occupiamoci del file /etc/conf.d/snmpd aggiungendo la riga:

```
-c /etc/snmp/snmpd.conf
```

alla variabile: *SNMPD_FLAGS* Dovrebbe quindi risultare qualcosa come questo:

```
SNMPD_FLAGS="-c /etc/snmp/snmpd.conf"
```

Ora facciamo partire il servizio *snmpd*:

```
/etc/init.d/snmpd start
/sbin/rc-update add snmpd default
```

Questa sintassi può variare da distribuzione a distribuzione. In questo caso ho utilizzato la sintassi di GNU/Linux Gentoo <http://www.gentoo.org/>. Se invece avessi utilizzato la sintassi GNU/Linux Slackware <http://www.slackware.com/>, avrei dovuto usare */etc/rc.d/rc.snmpd start*. Se fossimo in ambiente BSD, avremmo dovuto usare qualcosa come: */usr/local/etc/rc.d/snmpd.sh start* Percio accertatevi sul come avviare i servizi del vostro GNU/Linux o BSD (o system V) che sia, e continuate la lettura. Accertatevi anche che il path per il file MIB.txt sia corretto. Arrivati a questo punto dobbiamocominciare a configurare i vari servizi che vorremmo monitorare.
Primo fra tutti, il traffico generato. Lanciamo quindi il comando:

```
/usr/bin/cfgmaker  \
--output=/etc/mrtg/traffic.cfg \
--ifdesc=ip \
--ifref=descr \
--global "WorkDir: /var/www/localhost/mrtg" \
--global "Options[_]: bits,growright" \
public@localhost
```

In questo modo il comando cfgmaker creerà un file chiamato */etc/mrtg/traffic.cfg* che conterrà tutte le informazioni per il  polling snmp del traffico di rete. Occupiamoci ora della CPU

```
/bin/cat -s > /etc/mrtg/cpu.cfg
WorkDir: /var/www/localhost/mrtg
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.¬
txt
Target[localhost.cpu]:ssCpuRawUser. ¬
0&ssCpuRawUser.0:public@localhost
+ ssCpuRawSystem.0&ssCpuRawSystem.
0:public@localhost+ssCpuRawNice. ¬
0&ssCpuRawNic ¬ e.0:public@localhost
RouterUptime[localhost.cpu]: public@localhost
MaxBytes[localhost.cpu]: 100
Title[localhost.cpu]: CPU Load
PageTop[localhost.cpu]: <H1>Active CPU
Load%</H1>
Unscaled[localhost.cpu]: ymwd
ShortLegend[localhost.cpu]: %
YLegend[localhost.cpu]: CPU Utilization
Legend1[localhost.cpu]: Active CPU in % Load)
Legend2[localhost.cpu]:
Legend3[localhost.cpu]:
Legend4[localhost.cpu]:
LegendI[localhost.cpu]: Active
LegendO[localhost.cpu]:
Options[localhost.cpu]:growright,nopercent
```

Premiamo come poco fa i tasti [ctrl]+[d], e passiamo alla memoria:

```
/bin/cat -s > /etc/mrtg/mem.cfg
LoadMIBs: /usr/share/snmp/mibs/HOST-¬
RESOURCES-MIB.txt
Target[localhost.mem]: .1.3.6.1.4.1.2021.4.1¬
.0&.1.3.6.1.4.1.2021.4.11.0:public@localhost
PageTop[localhost.mem]: <H1>Free Memory </H1>
WorkDir: /var/www/localhost/mrtg
Options[localhost.mem]: nopercent,growright,¬
gauge,noinfo
Title[localhost.mem]: Free Memory
```

```
MaxBytes[localhost.mem]: 1000000
kMG[localhost.mem]: k,M,G,T,P,X
YLegend[localhost.mem]: bytes
ShortLegend[localhost.mem]: bytes
LegendI[localhost.mem]:  Free Memory:
LegendO[localhost.mem]:
Legend1[localhost.mem]: Free memory, not ¬
including swap, in bytes
```

Di nuovo [ctrl]+[d]. La memoria swap:

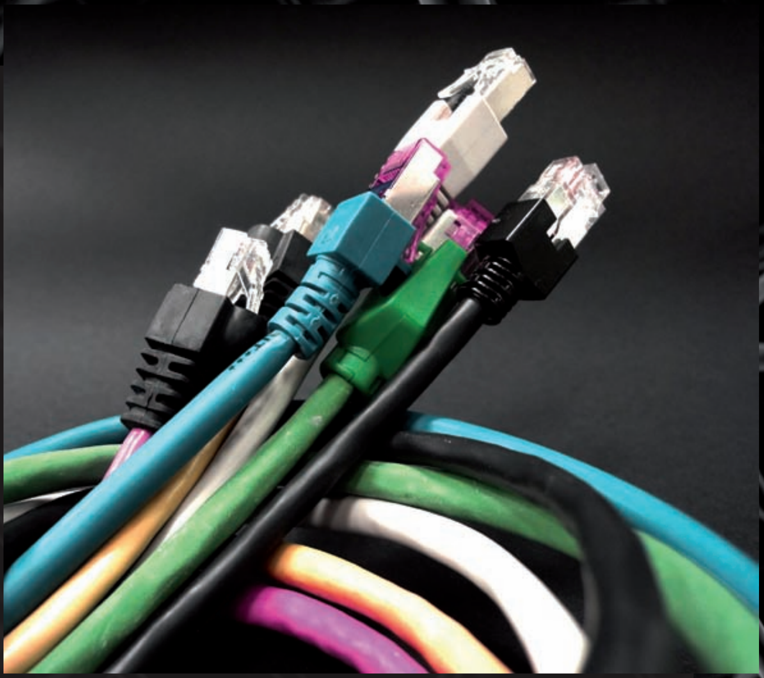
```
/bin/cat -s > /etc/mrtg/swap.cfg
LoadMIBs: /usr/share/snmp/mibs/UCD-¬
SNMP-MIB.txt
Target[localhost.swap]: memAvailSwap. ¬
0&memAvailSwap.0:public@localhost
PageTop[localhost.swap]: <H1>Swap Memory</H1>
WorkDir: /var/www/localhost/mrtg
Options[localhost.swap]: nopercent, ¬
growright,gauge,noinfo
Title[localhost.swap]: Free Memory
MaxBytes[localhost.swap]: 1000000
kMG[localhost.swap]: k,M,G,T,P,X
YLegend[localhost.swap]: bytes
ShortLegend[localhost.swap]: bytes
LegendI[localhost.swap]:  Free Memory:
LegendO[localhost.swap]:
Legend1[localhost.swap]: Swap memory ¬
avail, in bytes
```

E il consueto [ctrl]+[d]. Veniamo ora ad un classico del monitoraggio: il ping! Questo comodo tool ci permetterà di sapere i tempi di round trip su siti conosciuti da monitorare.

```
/bin/cat -s > /etc/mrtg/ping.cfg
WorkDir: /var/www/localhost/mrtg
Title[localhost.ping]: Round Trip Time
PageTop[localhost.ping]: <H1>Round Trip ¬
Time</H1>
Target[localhost.ping]: `/etc/mrtg/ping.sh`
MaxBytes[localhost.ping]: 2000
Options[localhost.ping]: growright, ¬
unknaszero,nopercent,gauge
LegendI[localhost.ping]: Pkt loss %
LegendO[localhost.ping]: Avg RTT
Legend1[localhost.ping]: Maximum Round ¬
Trip Time in ms
Legend2[localhost.ping]: Minimum Round ¬
Trip Time in ms
Legend3[localhost.ping]: Maximal 5 ¬
Minute Maximum Round Trip Time in ms
Legend4[localhost.ping]: Maximal 5 ¬
Minute Minimum Round Trip Time in ms
YLegend[localhost.ping]: RTT (ms)
```

Ancora [ctrl]+[d]. Cominciamo ora a generare gli script che andranno a richiamare mrtg:

```
/bin/cat -s > /etc/cron.mrtg/traffic.sh
```



```
#!/bin/sh
/usr/bin/mrtg /etc/mrtg/traffic.cfg
[ctrl]+[d]

/bin/cat -s > /etc/cron.mrtg/cpu.sh
#!/bin/sh
/usr/bin/mrtg /etc/mrtg/cpu.cfg
[ctrl]+[d]

/bin/cat -s > /etc/cron.mrtg/mem.sh
#!/bin/sh
/usr/bin/mrtg /etc/mrtg/mem.cfg
[ctrl]+[d]

/bin/cat -s > /etc/cron.mrtg/swap.sh
#!/bin/sh
/usr/bin/mrtg /etc/mrtg/swap.cfg
[ctrl]+[d]

/bin/cat -s > /etc/cron.mrtg/ping.sh
#!/bin/sh
/usr/bin/mrtg /etc/mrtg/ping.cfg
[ctrl]+[d]
```

Prepariamo ora lo script che andrà a compiere il comando: /bin/cat -s >

```
/etc/mrtg/ping.sh #!/bin/sh PING="/bin/ ¬
ping" # Google, for example
ADDR="google.com" DATA=`$PING -c10 -s500 ¬
$ADDR -q ` LOSS=`echo $DATA |
awk '{print $18 }' | tr -d %` echo $LOSS ¬
if [ $LOSS = 100 ]; then echo 0
else echo $DATA | awk -F/ '{print $5 }' fi.
```

Rendiamo quindi eseguibili gli script con:

```
/bin/chmod +x /etc/cron.mrtg/*.sh
/bin/chmod +x /etc/mrtg/ping.sh
```

A questo punto avviamo per tre volte ogni script, così da poter generare le prime statistiche. Non badate agli errori dato che inizialmente non avrà le vecchie (statistiche):

```
/bin/sh /etc/cron.mrtg/traffic.sh
/bin/sh /etc/cron.mrtg/cpu.sh
/bin/sh /etc/cron.mrtg/mem.sh
/bin/sh /etc/cron.mrtg/swap.sh
/bin/sh /etc/cron.mrtg/ping.sh
```

Finalmente abbiamo le nostre statistiche! Non ci resta infine che generare un index.html che permetta di ordinare tutti i nostri grafici:

```
/usr/bin/indexmaker --output=/var/www/ ¬
localhost/mrtg/index.html \
--title="Power Under Control :)" \
--sort=name \
--enumerate \
/etc/mrtg/traffic.cfg \
/etc/mrtg/cpu.cfg \
/etc/mrtg/mem.cfg \
/etc/mrtg/swap.cfg \
/etc/mrtg/ping.cfg
```

Perfetto! Non ci resta che aggiungere in cron il nostro lavoro:

```
crontab -e
```

```
/bin/cat >> /var/spool/cron/crontabs/root
*/5 * * * * /bin/run-parts /etc/cron. ¬
mrtg 1> /dev/null
```

Bene. Abbiamo concluso!! Puntiamo il nostro browser preferito su: /var/www/localhost/www/index.html In caso qualcuno di voi volesse usare mini_httpd o apache, sar√† è necessario far puntare la DocumentRoot a tale subdirectory, avviare il servizio e collegarsi su: http://localhost/mrtg Ecco qui le nostre statistiche! Per approfondire meglio lo studio dell'snmp, il tool *net-snmp* mette a disposizione svariati tool informativi e di diagnosi. Iniziamo con snmpwalk: Snmpwalk is an SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information Quindi, snmpwalk, sfrutta la richiesta *GETNEXT* per ottenere informazioni sull'alberatura snmp dell'oggetto richiesto. In questo modo possiamo utilizzarlo come banale "visualizzatore" di stato. Il risultato ottenuto sarà quindi il valore dell'OID (Object Identifier) richiesto. Cominciamo quindi con la richiesta dell'oggetto: *mgmt.1.2.2.1.10.2*

```
$ snmpwalk -v 1 -c public localhost ¬
mgmt.1.2.2.1.10.2
IF-MIB::ifInOctets.2 = Counter32: 140021440
```

Ecco che quindi, snmpwalk, ci ha restituito il valore dell'oggetto desiderato. Per conoscere a cosa corrisponde un determinato oggetto, possiamo usare un'altra utility messa a disposizione dalla suite net-snmp *snmptranslate*. Come è facile intuire, questo programma trasforma l'oggetto (OID) in una descrizione sul suo contenuto, facilitando così la lettura e la comprensione.

```
$ snmptranslate -IR -Td mgmt.1.2.2.1.10.2
IF-MIB::ifInOctets.2
ifInOctets OBJECT-TYPE
  -- FROM       IF-MIB, RFC1213-MIB
  SYNTAX        Counter32
  MAX-ACCESS    read-only
  STATUS        current
```

DESCRIPTION "The total number of octets received on the interface, including framing characters.
Discontinuities in the value of this counter can occur at re-initialization of the management system,
and at other times as indicated by the value of ifCounterDiscontinuityTime."

```
::= { iso(1) org(3) dod(6) internet(1) ¬
mgmt(2) mib-2(1)
 interfaces(2) ifTable(2) ifEntry(1) ¬
ifInOctets(10) 2 }
```

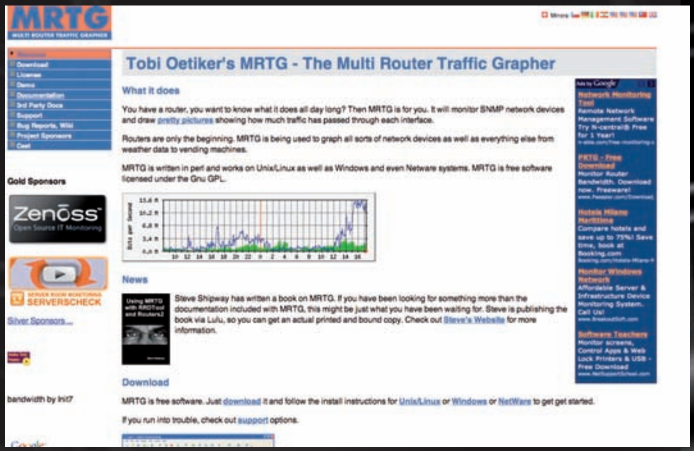
Ora, per esempio, potreste divertirvi a conoscere gli OID di un vostro host, semplicemente con:

```
$ snmpwalk -v 1 -c public localhost
```

Quindi, adesso, potrete generare i vostri file di configurazione (oppure come ho fatto io per il ping, con uno script) a seconda delle informazioni di cui avete bisogno. Una lettura ai manuali di:

mrtg
snmpd
snmpwalk
snmptranslate

sarà sicuramente più esplicativa. Beh, non mi resta che augurarvi un buon *MRTG* a tutti! khazad-dum.







di Raffaele Rambaldi
Raffaele_Rambaldi@hotmail.com

# SNIFFING

SERIAL ATTACK

**LO STRATO PIÙ BASSO DELL'INFRASTRUTTURA DI RETE È SPESSO IGNORATO DAGLI UTENTI CHE NON INTERAGISCONO CON ESSO. SENZA CONSIDERARE DELIBERATAMENTE QUESTO LIVELLO È IMPOSSIBILE COSTRUIRE UN SISTEMA SICURO PER LE APPLICAZIONI CHE AGISCONO A LIVELLI PIÙ ELEVATI.**

## IO SNIFFO, TU SNIFFI, EGLI SNIFFA

Sniffare è un'azione passiva ossia vengono elaborati solo i dati che raggiungono autonomamente lo "sniffer". Vuol dire che i dati devono viaggiare autonomamente perché non viene fatta alcuna azione per andarseli a prendere.
Il concetto è fondamentale perché generalmente le reti sono segmentate da innumerevoli apparati, come ad esempio gli switch, che creano circuiti virtuali tra i nodi, oppure da router che smistano i pacchetti soltanto sul nodo di competenza.
Se volessimo analizzare il traffico generato da un server collegato direttamente ad uno switch layer 2 o layer 3, che oggigiorno è la regola, occorrerebbe replicare in mirroring la porta del collegamento del server su di una seconda porta dello switch dove collocare lo sniffer.
In tal modo tutti i dati che transitano sui circuiti virtuali tra i diversi nodi gestiti dallo switch, che altrimenti sarebbero invisibili, possono essere rilevati.
Per questa ragione, se pensiamo di utilizzare uno sniffer da casa, a valle di una linea ADSL, per scoprire chissà quale segreto, probabilmente resteremmo delusi.
Di contro, utilizzare uno strumento simile al lavoro o all'Università potrebbe essere visto come un attacco all'integrità del sistema e se le policy aziendali prevedono il licenziamento, attenzione a non farvi beccare!
Ciò non toglie che uno sniffer può rivelarsi uno strumento insostituibile per capire in che modo comunicano in rete le applicazioni che normalmente utilizziamo, ma andiamo con ordine.

## LIVELLI ED INDIRIZZI

Secondo il modello ISO/OSI di riferimento, tutte le interfacce che insistono sulla medesima rete ethernet hanno un indirizzo fisico al livello più basso che normalmente è differente dall'indirizzo utilizzato dal protocollo, che si chiama MAC address. Oltre a questo, tutti i nodi dispongono di un indirizzo di broadcast univoco per tutto il segmento di rete. Nel normale funzionamento della scheda di rete, viene elaborato solamente il pacchetto che contiene il proprio indirizzo fisico o quello di broadcast, ignorando tutti gli altri.
Lo sniffer, invece, raccoglie tutto. Essenzialmente presenta all'utente una sequenza ordinata di pacchetti che contengono principalmente l'ora in cui sono stati ricevuti, l'indirizzo sorgente, l'indirizzo di destinazione ed il contenuto.

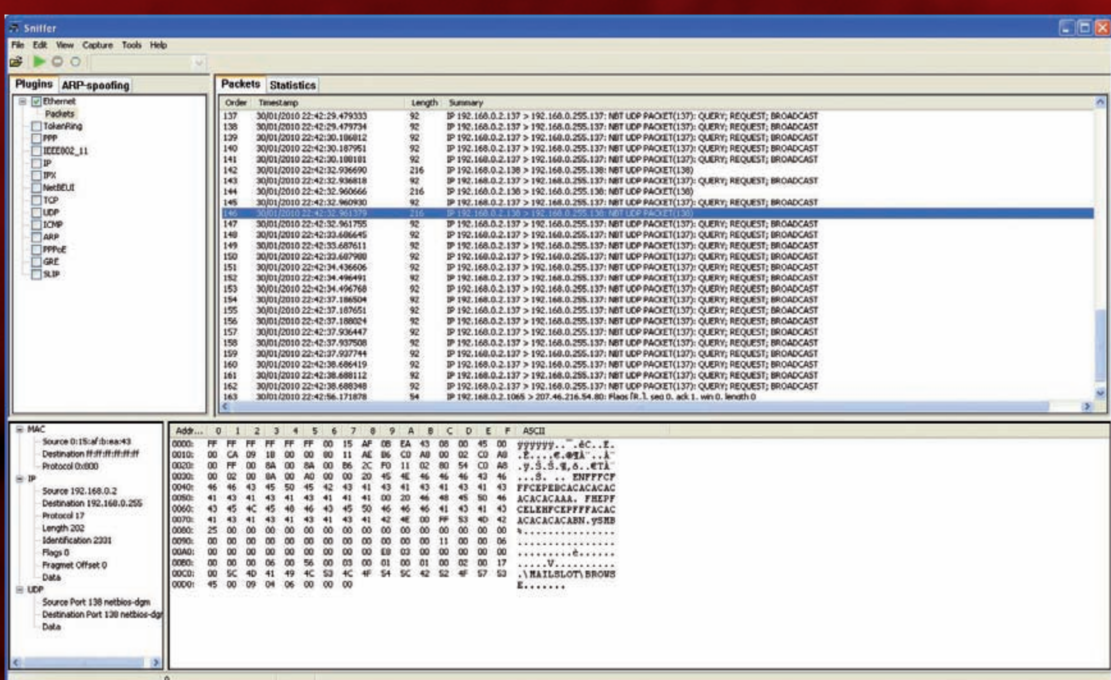
**SNIFFING, TRADOTTO ALLA LETTERA, SIGNIFICA "ANNUSARE, ODORARE". ED È PROPRIO IL TERMINE PIÙ ADATTO PER INDICARE L'AZIONE DI RILEVARE DATI CHE NON SONO DESTINATI ALLA PROPRIA MACCHINA, MA SEMPLICEMENTE IN TRANSITO. "SNIFFANDO" CI SI LIMITA AD ELABORARE I PACCHETTI CHE RAGGIUNGONO IL PROPRIO NODO CHE NORMALMENTE VERREBBERO SCARTATI, SENZA ALTERARNE IL CONTENUTO. QUALORA QUEST'ULTIMO VENGA ALTERATO SI TRATTEREBBE DI "SPOOFING", DEL QUALE PARLEREMO PROSSIMAMENTE. I PROGRAMMI PER FARE SNIFFING SONO MOLTI E NON ABBIAMO LO SPAZIO DI ANALIZZARLI NEL DETTAGLIO MA I MIGLIORI SONO REPERIBILI ALL'INDIRIZZO HTTP://SECTOOLS.ORG/SNIFFERS.HTML, CORREDATI ANCHE DI UN'ESAUSTIVA DESCRIZIONE DELLE FUNZIONALITÀ DI CIASCUNO.**

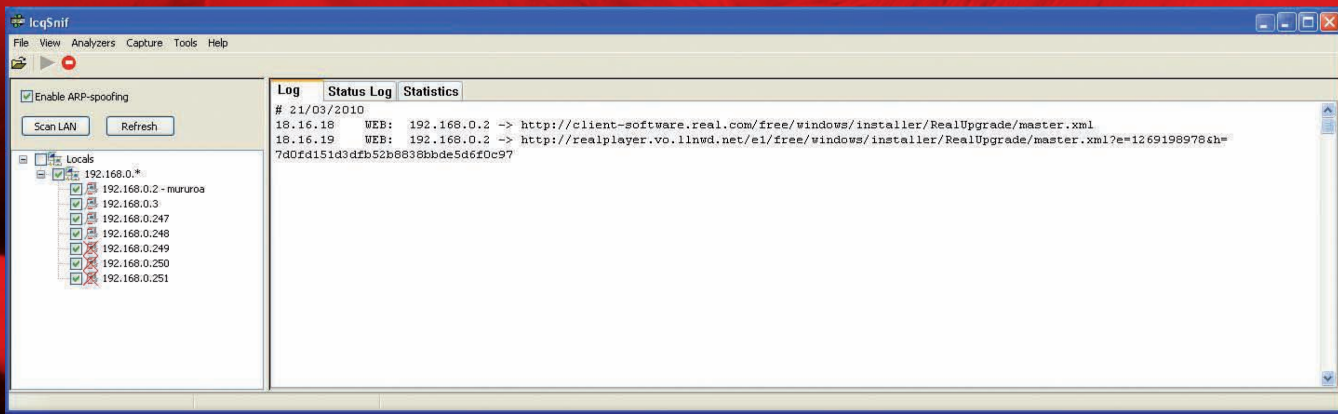
Avendo a disposizione una sequenza di questo tipo è possibile ricostruire il traffico tra i diversi nodi ma occorre disporre di un discreto spazio sul disco perché in alcune realtà possono transitare migliaia di pacchetti al secondo che, se consideriamo che ciascuno occupa almeno 64 byte, si capisce come si possa rapidamente generare una quantità esagerata di informazioni.

Normalmente proprio per questa ragione è meglio utilizzare dei filtri con i quali limitarsi a catturare esclusivamente quei pacchetti che realmente reputiamo degni di interesse.

## MA COSA SNIFFO?

L'attività più difficoltosa nell'uso di uno sniffer è decidere che cosa catturare. Occorre avere una profonda conoscenza dei meccanismi dei diversi protocolli di rete e non solo del TCP/IP.
Per prima cosa decidiamo che cosa catturare e stabiliamo a che livello della pila ISO/OSI vogliamo lavorare.
Al primo livello possiamo raccogliere i segnali Bluetooth, DSL, RS-232 ed altri, mentre nel secondo livello possiamo raccogliere i segnali Ethernet,






PPP, Frame Relay, Token Ring, Wi-Fi, ATM ed altri. In entrambi i livelli dobbiamo avere a disposizione una sonda particolare in grado di interpretare tali segnali. Nel nostro caso consideriamo unicamente la rete ethernet perché possiamo utilizzare come sonda la scheda ethernet del nostro computer.
Sulla rete ethernet, al terzo livello, esistono vari protocolli alternativi all'IP (Internet Protocol) che conosciamo così bene. Ad esempio possiamo citare i protocolli IPX, X.25 e DHCP solo per indicare i principali.
Non si tratta di teoria. In pratica una stampante con interfaccia di rete configurata male, collegata sullo switch di casa, potrebbe generare traffico IPX assolutamente inutile. Se collegate uno sniffer e rilevate traffico IPX o Appletalk senza avere un MacIntosh, qualcosa non quadra.
Salendo al quarto livello possiamo rilevare pacchetti TCP o UDP, usati su IP, ma anche SPX se è presente l'IPX oppure il vecchio e glorioso NetBIOS, ormai in progressivo abbandono.
Al livello più alto, applicativo, rileviamo i protocolli DNS, NPT, SNMP, POP, IMAP, FTP, IRC, HTTP, fino ad arrivare ai protocolli più oscuri utilizzati da applicazioni di nicchia.

## ABBIAMO LE IDEE CHIARE?

E' proprio al livello applicativo che c'è il succo di quello che vogliamo scoprire. Arrivati a questo punto, possiamo citare tantissima letteratura che ci suggerisce come fare a rilevare le password, i numeri di carta di credito oppure dati privati che dovrebbero restare nascosti.
Se consideriamo ad esempio il Telnet, impostando i filtri su host server ed host client possiamo limitarci a catturare il traffico in transito sulla porta 23 del TCP. All'inizio della sessione tra server e client avremo così modo di catturare la sequenza di caratteri che contiene l'utente e password praticamente senza fare alcuno sforzo.
In effetti, sono tutte cose tecnicamente molto semplici da realizzare attraverso l'uso di uno sniffer, ma non dimentichiamo che i dati ci devono passare davanti. Infatti sapere che il Telnet trasmette le password di autenticazione in chiaro un carattere alla volta, ci serve a poco se quei caratteri non passano davanti alla scheda ethernet sulla quale insiste lo sniffer. Non dimentichiamo, inoltre, che i vecchi sistemi di comunicazione come Telnet e POP3, sono in progressivo abbandono a favore di sistemi molto più avanzati come SSL, HTTPS, Kerberos e simili, per i quali il discorso delle password in chiaro non vale più. Nonostante tutto, lo sniffer è uno strumento impareggiabile quando si vuole risolvere un problema di comunicazione. Sapere nel dettaglio che cosa si dicono due applicazioni attraverso la rete può essere molto utile soprattutto per coloro che sviluppano le applicazioni e vogliono implementare meccanismi di traffico sempre più performanti.

di Giovanni Federico
giovanni.federico@isek.it

PARTE II

# HOST-BASED INTRUSION DETECTION & LOG MONITORING

# OSSEC

SICUREZZA

**Si conclude in queste pagine il discorso intrapreso nello scorso numero della rivista relativo ad OSSEC, uno tra i più evoluti HIDS offerti dalla comunità del software libero. Buona lettura!**

L'Conclusa la necessaria trattazione teorica nel corso del precedente numero della rivista, in questa sede vedremo come rendere definitivamente operativa la soluzione prospettata.
Prima di iniziare stendiamo una rapida roadmap di quel che andremo a fare di seguito.
In prima battuta, com'è facile intuire, ci preoccuperemo di installare OSSEC sul server (che ricordiamo essere OpenBSD 4.6) configurandolo fedelmente rispetto a quanto detto nella precedente puntata.
Sarà inoltre comodo installare l'interfaccia web (ossec-wui) direttamente in questo passaggio, rendendola immediatamente funzionale.
Vedremo quindi come abilitare effettivamente i processi di difesa autonomi attraverso la modalità "Active Response" dell'HIDS e come configurare la stessa con il firewall di sistema (PF). Passeremo quindi all'installazione dei vari agenti sugli host della nostra rete.
Infine, testeremo il lavoro svolto pianificando alcuni attacchi generici diretti sia al server che ai vari host.

## INSTALLAZIONE DEL SERVER

Nel numero 197 della rivista abbiamo avuto modo di analizzare l'installazione di OpenBSD 4.6. Partiremo pertanto da quella nel seguito di questo articolo, integrando le opportune modifiche da apportare al sistema.

Al momento della scrittura di questo articolo, l'ultima versione di OSSEC disponibile per il download è la 2.3 reperibile all'indirizzo www.ossec.net/main/downloads/.

Logghiamoci pertanto come root al server OpenBSD, scarichiamo e decomprimiamo l'archivio di nostro interesse nella directory di root di Apache (/var/www, il motivo di questa scelta sarà chiaro quando affronteremo l'installazione dell'interfaccia Web dell'applicativo):

```
# cd /var/www/
# wget http://www.ossec.net/ ¬
files/ossec-hids-2.3.tar.gz
# tar zxvf ossec-hids-2.3.tar.
gz
```

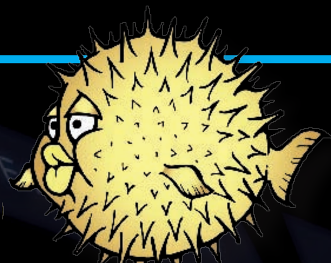
Avviamo quindi il processo di installazione, che commenteremo di seguito in ogni singolo punto:

```
# cd ossec-hids-2.3/
# ./install.sh
```

Verrà prima di tutto richiesta la lingua da utilizzare per l'installazione; digitiamo "it" e diamo Invio.
Lo script di installazione (di seguito SDI) si occuperà di fornire un riepilogo del sistema, chiedendoci conferma per continuare. Diamo semplicemente Invio per procedere.

Da questo punto in poi partiranno una serie di domande da parte dello SDI volte a definire la tipologia di installazione richiesta, eventuali parametri relativi alla nostra macchina e le directory dove finalizzare il setup. Malgrado questa fase si spieghi da sola, commenteremo anche qui i singoli passaggi:

Definiamo innanzitutto la tipologia di installazione tra quelle proposte. Scriviamo pertanto "server" e diamo Invio.
Indichiamo il percorso di installazione dell'HIDS. Scriviamo "/var/www/ossec".



Abilitiamo la notifica degli alert via mail rispondendo "s".
Inseriamo il nostro indirizzo di posta elettronica
Lo SDA individuerà autonomamente il server SMTP relativo alla mail inserita, confermiamo l'utilizzo del medesimo scrivendo "s".
Abilitiamo il controllo di integrità dei file (Syscheck) digitando "s".
Stesso discorso per il riconoscimento dei rootkit (Rootcheck).
Attiviamo la risposta attiva (Active Response) rispondendo affermativamente all'apposita richiesta ed a quella successiva relativa alle risposte firewall-drop.
Definiamo eventuali IP (esclusi i DNS primari e secondari, già inclusi) da escludere dai controlli. Nel nostro caso, volendo monitorare anche i comportamenti interni alla rete, abbiamo risposto negativamente.
Disabilitiamo il Syslog remoto rispondendo "n".

Il processo di configurazione pre-installazione è ora concluso.

Immediatamente l'HIDS offre un riepilogo dei file che saranno oggetto di analisi sulla macchina entro quale è installato.
Il processo è totalmente automatizzato e lo SDA individua del tutto autonomamente i file di log di base del sistema, nel nostro caso OpenBSD:

```
3.6- Imposto la configurazio-
ne per l'analisi dei seguenti
logs:
-- /var/log/messages
-- /var/log/authlog
-- /var/log/secure
-- /var/log/xferlog
-- /var/log/maillog
-- /var/www/logs/access_log ¬
(apache log)
-- /var/www/logs/error_log ¬
(apache log)
```

Diamo Invio per dare il via all'effettiva compilazione dei sorgenti dell'applicativo.
Il processo si esaurirà nel giro di qualche minuto.
Se tutto è andato per il verso giusto l'output risultante dello SDA dovrebbe essere il seguente:

```
<...>
- Configurazione terminata cor-
rettamente.
       - Per avviare OSSEC
HIDS: /var/www/ossec/bin/ ¬
ossec-control start
       - Per arrestare OS-
SEC HIDS:/var/www/ossec/bin/ ¬
ossec-control stop
- La configurazione può essere
vista o modificata in /var/ ¬
www/ossec/etc/ossec.conf
Grazie per aver scelto OSSEC
HIDS.
<...>
```

Concludiamo infine l'installazione dell'applicativo impostando l'avvio dello stesso insieme al sistema operativo, inserendo nel file "/etc/rc.local" la seguente direttiva:

```
echo "Avvio OSSEC HIDS"
/var/www/ossec/bin/ossec-¬
control start
```

## RISPOSTA ATTIVA E CONFIGURAZIONE DI PF

Installato OSSEC ci preoccuperemo di configurare correttamente PF, integrandolo all'HIDS al fine di rendere operativa la modalità Active Response dell'applicativo.

Nel numero 188 della rivista abbiamo avuto modo di affrontare abbastanza dettagliatamente l'utilizzo e la configurazione del packet filter di OpenBSD per utilizzi generici. In questa sede, partendo da quella base, aggiungeremo un'ulteriore necessaria nozione che ci consentirà di capire come funziona l'interfacciamento tra l'HIDS ed OpenBSD.

Per gestire più istanze singole accorpandole ad un'unica azione, PF offre un meccanismo tabellare semplice e performante. Definendo apposite tabelle di indirizzi identificate da un nome univoco, è infatti possibile associare particolari azioni al blocco di indirizzi identificato dalle stesse.

OSSEC sfrutta proprio questa caratteristica. Inserendo un'opportuna tabella denominata "ossec_fwtable" all'interno del file di configurazione del firewall l'applicativo si occuperà di riempirla secondo le necessità del caso, andando di volta in volta ad inserire quei singoli IP identificati quali mittenti degli alert generati e dei tentativi di attacco ricevuti.

PF, matchando semplicemente la tabella, imposterà un blocco in uscita ed in entrata su tutto il gruppo di IP definito.

Vediamo quindi come istruire il firewall in tal senso. Editiamo la configurazione dello stesso, inserendo nel file "/etc/pf.conf" le seguenti tre righe:

```
# OSSEC ----------------------
------------
table <ossec_fwtable> persist
block in quick from <ossec_ ¬
fwtable> to any
block out quick from any to ¬
<ossec_fwtable>
# ----------------------------
-------------
```

Non importa la collocazione di questo blocco di istruzioni. Questo perché, come abbiamo avuto modo di scoprire illo tempore, l'utilizzo della direttiva quick impone l'esecuzione dell'azione definita indipendentemente dall'ordine che questa assume rispetto alle altre.

Da questo momento l'HIDS si integrerà perfettamente al firewall del sistema.
I meccanismi di protezione autonoma offerti faranno si che l'applicativo, d'ora in poi, si configuri esattamente come HIPS (Host-based Intrusion Prevention System).

La modalità Active Response di OSSEC non si esaurisce al solo inserimento degli IP originari degli attacchi nella tabella appena definita. Essa, di default, per un periodo di tempo determinato in fase di scrittura delle regole dell'HIPS, collocherà i medesimi IP nel file "hosts.deny" del sistema, su OpenBSD come per la stragrande maggioranza dei sistemi Unix-like, collocato nella directory "etc".

## AGENTI

Come abbiamo esaurientemente spiega-

to nel corso del numero passato, OSSEC colleziona le informazioni ed i log degli host della nostra rete attraverso i vari agenti installati sulle singole macchine.

Per funzionare, un agente invia la propria chiave di autenticazione al Server che lo identifica univocamente.
Il tool che si occupa della gestione degli agenti è “manage_agents”, collocato nella directory “/var/www/ossec/bin/”.

Vediamo di seguito il procedimento per l’inserimento di un singolo agente; questo, ovviamente, risulterà invariato per ogni ulteriore installazione. In prima istanza, una volta avviato il tool, digitiamo “A” per aggiungere un nuovo client:

```
# /var/www/ossec/bin/manage_
agents
...
    (A)dd an agent (A).
    (E)xtract key for an ¬
agent (E).
    (L)ist already added ¬
agents (L).
    (R)emove an agent (R).
    (Q)uit.
Choose your action: A,E,L,R or
Q: A
```

Saranno quindi richiesti i dettagli relativi al nuovo agente (nome, indirizzo IP ed un ID numerico).
Rispondiamo in base alle nostre esigenze come di seguito:

```
...
* A name for the new agent: ¬
PC-Windows1
* The IP Address of the ¬
new agent: 192.168.1.100
* An ID for the new agent ¬
[001]: 001
...
Confirm adding it?(y/n): y
```

Il tool ritornerà quindi all’interfaccia iniziale. Stavolta digitiamo “E” per generare la chiave di autenticazione per l’agente appena creato. Anche in questo caso il procedimento è guidato:

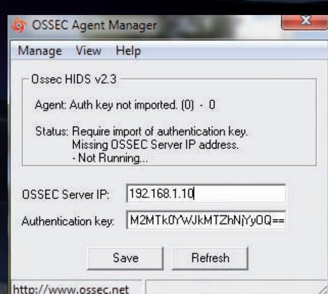
```
Choose your action: A,E,L,R ¬
or Q: E
Available agents:
    ID: 001, Name: PC-¬
Windows1, IP: 192.168.1.100
Provide the ID of the agent ¬
to extract the key (or ‘\q’ ¬
to quit): 001

Agent key information ¬
for ‘001’ is:
MDAxIFBDLVdpb ...
```

La chiave appena generata sarà quella di volta in volta richiesta in fase di installazione dell’agente sui vari host della rete. Per ogni nuovo client ne genereremo una ad hoc.

## WINDOWS AGENTS

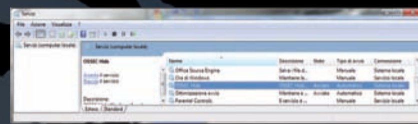
Per Microsoft Windows l’eseguibile da scaricare ed installare lo troviamo all’indirizzo www.ossec.net/files/ossec-agent-win32-2.3.exe.
In fase di installazione abilitiamo l’integrity checking e disabilitiamo il monitoring dei log di IIS (fatti salvi i casi in cui vi sia effettiva necessità, ad esempio nell’ipotesi in cui il nostro host Windows fosse un ulteriore od il singolo server web).
Conclusa l’installazione in classico ed inconfondibile stile Microsoft (Avanti, Avanti, Fine) si presenterà di fronte ai nostri occhi l’Agent Manager. In questa schermata dovremo inserire l’indirizzo IP del server OSSEC e l’Auth Key.



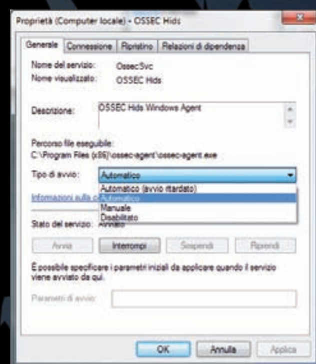

*L’OSSEC Agent Manager su Microsoft Windows in fase di abilitazione dell’host come Agente dell’HIPS.*

La pressione del tasto Save ed un click su Manage -> Start OSSEC è più che sufficiente per far sì che l’agente assuma vita autonoma.

Per abilitare l’agente direttamente all’avvio del sistema modifichiamo attraverso services.msc il servizio “OSSEC Hids Windows Agent” impostando il Tipo di Avvio su “Automatico”.



*Abilitiamo l’avvio automatico dell’Agente modificando l’apposito valore.*




A questo punto la postazione Windows appena configurata farà parte della rete OSSEC.
Per testare l’effettiva operatività dell’agente, dal server digitiamo:

```
# /var/www/ossec/bin/agent_ ¬
control -lc
OSSEC HIDS agent_control. ¬
List of available agents:
    ID: 000, Name: www. ¬
gfhome.info (server), IP: ¬
127.0.0.1, Active/Local
    ID: 001, Name: PC-Windows1,¬
IP: 192.168.1.100, Active
```

## UNIX AGENTS

Il procedimento di seguito illustrato riguarderà l’installazione dell’agente su host Linux, BSD, Solaris e Mac.
La distro utilizzata in quest’esempio è Gentoo. Resta inteso che questo dettaglio è di scarso interesse in quanto il processo qui descritto sarà lo stesso per qualsiasi distribuzione.

Il pacchetto da scaricare sarà quello usato in fase di installazione del server. Semplicemente, appena richiesto, definiremo come “agent” il tipo di installazione desiderata:

```
[root@pluto ~]# wget http://
¬ www.ossec.net/files/ossec-¬
hids-2.3.tar.gz
[root@pluto ~]# tar zxvf ¬
ossec-hids-2.3.tar.gz
[root@pluto ~]# cd ossec-¬
hids-2.3/
[root@pluto ossec-hids-2.3]#
¬./install.sh
```

Come fatto per il server selezioniamo l'italiano come lingua per l'installazione e procediamo.
Commenteremo di seguito ogni singolo passaggio dell'installazione:

Digitiamo "agent" alla richiesta del tipo di installazione da effettuare.
Stavolta definiamo "/var/ossec" la directory entro cui installare l'agente.
Inseriamo l'indirizzo IP del server OSSEC (nel nostro caso 192.168.1.10).
Attiviamo syscheck, rootcheck ed Active Response digitando "s" a tutte le richieste.
Diamo invio per concludere la configurazione e dare inizio alla compilazione.

Dopo qualche istante, a compilazione completata, dovremmo ricevere in output le seguenti informazioni relative all'installazione appena effettuata:

```
...
- Configurazione terminata cor-
rettamente.
- Per avviare OSSEC HIDS: /var¬
/ossec/bin/ossec-control start
- Per arrestare OSSEC HIDS: ¬
/var/ossec/bin/ossec-control
stop
- La configurazione può essere
vista o modificata in /var/ ¬
ossec/etc/ossec.conf
Grazie per aver scelto OSSEC
HIDS.
...
```

Impostiamo quindi l'avvio dell'agente al boot inserendo "/var/ossec/bin/ossec-control start" nell'apposito file di init della nostra distribuzione.

Installato l'agente sull'host generiamo, come visto prima, un'ulteriore chiave di autenticazione per il Client appena configurato. Fatto questo, abilitiamo l'host utilizzando anche sull'agente "manage_agents":

```
[root@pluto ossec-hids-2.3]# /var/ossec/
bin/manage_agents
...
(I)mport key from the ¬
server (I).
(Q)uit.
Choose your action: I or Q: I
...
Paste it here (or '\q' to ¬
quit): MDAyIFBDLUxpbnV4MSAx...
...
Confirm adding it?(y/n): y
Added.
```

Avviamo pertanto il Client:

```
[root@pluto ossec-hids-2.3]# ¬
/var/ossec/bin/ossec-¬
control start
Starting OSSEC HIDS v2.3 ¬
(by Trend Micro Inc.)...
Started ossec-execd...
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

Dal server testiamo, infine, l'operatività dell'agente:

```
# /var/www/ossec/bin/agent_ ¬
control -lc
OSSEC HIDS agent_control. ¬
List of available agents:
   ID: 000, Name: www.gfhome.¬
info (server), IP: 127.0.0.1, ¬
Active/Local
   ID: 001, Name: PC-Windows1,¬
IP: 192.168.1.100, Active
   ID: 002, Name: PC-Linux1, ¬
IP: 192.168.1.132, Active
```

Ripetendo sia il procedimento illustrato qui che quello per Agenti Windows, metteremo via via tutti i nostri host sotto l'occhio vigile di OSSEC.

## OSSEC WUI

Leggere gli alert via posta elettronica e via terminale farà sicuramente molto nerd ma nel caso di reti complesse e caratterizzate dalla presenza di innumerevoli host non è decisamente la scelta più comoda.

Avere l'opportunità di utilizzare un'interfaccia che riassuma lo stato del network ci risparmierà indubbiamente molto tempo, consentendoci, peraltro, di avere un quadro d'insieme della situazione aggiornato in tempo reale e visibile in ogni parte del globo.

Seguendo quindi la roadmap prefissata, occupiamoci di installare il frontend web di OSSEC sfruttando Apache.

I più attenti si ricorderanno che OpenBSD gestisce Apache in un ambiente totalmente isolato dal resto del sistema (chroot). Da qui, piuttosto che utilizzare un numero considerevole di link simbolici, abbiamo preferito installare OSSEC direttamente nella root del server Web (/var/www).
Questo ci permetterà di rendere l'installazione della WUI molto più snella, non dovendoci preoccupare dell'impossibilità da parte di Apache di accedere a directory esterne al suo environment di lavoro.

Scarichiamo quindi il tarball dell'interfaccia Web (al momento della scrittura di questo articolo giunta alla versione 0.3) ed installiamola sul Server:

```
# cd /var/www/htdocs/
# wget http://www.ossec.net/fi ¬
les/ui/ossec-wui-0.3.tar.gz
# tar zxvf ossec-wui-0.3.tar.gz
```

Avviamo lo script di setup per impostare l'autenticazione richiesta quando accediamo alle pagine della WUI:

```
# cd ossec-wui-0.3
# ./setup.sh
Setting up ossec ui...
Username: giovanni
New password:
Re-type new password:
Adding password for user ¬
giovanni
Setup completed successfuly.
```

Modifichiamo ora il file di configurazione (ossec_conf.php), indicando il percorso di OSSEC che nel nostro caso sarà, proprio per le constatazioni relative all'am-

biente chroot fatte prima, “/ossec”.
Viste le nostre necessità la restante parte della configurazione è più che sufficiente: la lasceremo pertanto invariata. In definitiva il file dovrà risultare così:

```
$ossec_dir=" /ossec";
$ossec_max_alerts_per_page ¬
= 1000;
$ossec_search_level = 7;
$ossec_search_time = 14400;
$ossec_refresh_time = 90;
```

Un rapido collegamento con un qualunque browser al server web (nel nostro caso 192.168.1.10) all’indirizzo http://~/ossec-wui-0.3/index.php ci confermerà immediatamente la riuscita dell’installazione.




*L’homepage della WUI ci mostra un riepilogo degli ultimi eventi e log analizzati e dei file modificati (integrity check).*

La struttura della WUI è piuttosto semplice. Essa si avvale di un’interfaccia suddivisa in 5 schede: Main, Search, Integrity checking, Stats, About. Escludendo l’ultima, ognuna di queste offre preziose informazioni relative ai dati raccolti da OSSEC e dai vari agenti nella nostra rete.

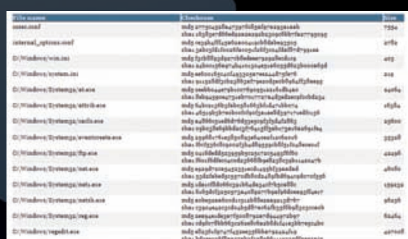
Nella home è proposto un quadro d’insieme dove sono visualizzati gli ultimi alert, la lista degli agenti attivi disponibili e gli ultimi file modificati (integrity check).
Su quest’ultimo punto spenderemo qualche parola. Durante il processo di installazione degli agenti e del server stesso, i file “caldi” del sistema sono tutti firmati digitalmente dall’applicativo. In sostanza è generata una coppia di hash (SHA1 ed MD5) associata ai singoli file predetti che li identifica in modo univoco insieme al loro contenuto.

La modifica di questi ultimi, volontaria o meno che sia (si pensi ad esempio per Windows all’operato di trojan, virus, etc. e per Linux a backdoor, exploit et similia), determinerà necessariamente la generazione di un hash diverso, evidenziando l’avvenuto cambiamento.

È proprio su questo elementare presupposto che si basa il controllo di integrità (integrity checking) condotto da OSSEC.

Nell’esempio proposto in figura, relativo alla scheda “Integrity checking” della WUI, possiamo appunto osservare il checksum fatto al primo avvio dall’agente ospitato sul PC montante Microsoft Windows.

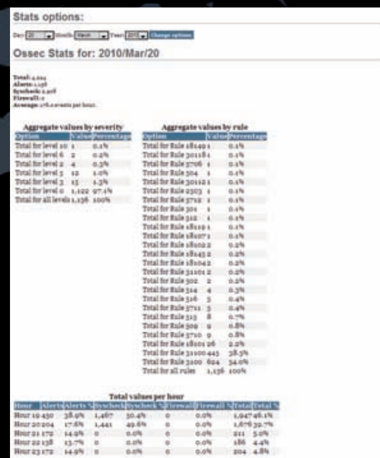
A sinistra è indicato il file monitorato, al centro è possibile visualizzare la coppia di hash associata allo stesso ed a destra la dimensione.



*Il controllo di integrità dei file analizzati dall’agente montato su Windows.*

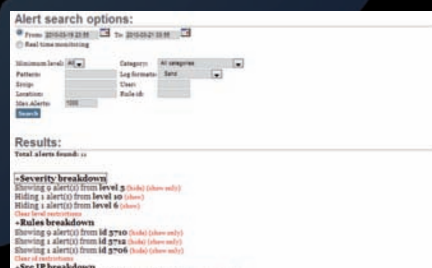
In caso di modifica degli stessi, naturalmente, sarà generato un apposito alert informativo. Anche se la probabilità di falsi positivi in questo contesto è molto alta, è sempre auspicabile prestare particolare attenzione a questo genere di alert in quanto potrebbe rappresentare, con buona approssimazione, un primo campanello di allarme circa la compromissione del nostro host da parte di malware generico.

La scheda “Stats” ci offre in una singola schermata le statistiche degli alert generati dall’HIPS suddivise per livelli, regole ed orari. Rappresenta pertanto, indubbiamente, un ottimo strumento per avere una visione d’insieme della situazione del nostro network in tempo reale.




*Le statistiche degli alert generati rappresentano un ottimo strumento offerto al net admin per monitorare costantemente la situazione generale dell’intera rete.*

Infine, nella scheda “Search”, è possibile ricercare singoli eventi ed alert generati. Nell’esempio proposto in figura abbiamo focalizzato la nostra attenzione su SSH.




*La funzionalità di ricerca consente di visualizzare unicamente gli alert di nostro interesse.*

## 3, 2, 1... CIAK, AZIONE!

Dopo questo excursus tra configurazioni ed installazioni è giunto il momento di testare sul campo l’affidabilità della soluzione OSSEC. Fedelmente a quanto analizzato nel corso dell’intero articolo effettueremo alcuni attacchi contemplati dalle regole analizzate.

Oggetto di nostro interesse in questa sede saranno pertanto i riscontri ai seguenti:

Tentativi di accesso non autorizzati (di

seguito TANA) su protocollo SSH.
Scanning effettuati con Nikto a website e web apps.
Segfault di applicativi su Windows.
Controlli di integrità su Windows.

Per ognuno dei punti succitati analizzeremo il comportamento di OSSEC constatando anche come l'operato di Active Response stronchi sul nascere qualsiasi tentativo di attacco ai sistemi, coordinandosi in modo perfettamente autonomo con PF ed OpenBSD.

## 1 - TANA SU PROTOCOLLO SSH

Per testare il comportamento di OSSEC in caso di attacchi brute force al protocollo SSH utilizzeremo uno dei tantissimi script disponibili online: mtsshbrute.py che trovate disponibile per il download sul nostro sito.

Lo script, scritto in python, consente di inoltrare multiple richieste di accesso in base ad utenti e password definite in appositi file che fungono da dizionario. Supportando il threading inoltre ci consente di velocizzare di molto l'operato.

Avviamo pertanto lo script come di seguito:

```
$ python mtsshbrute.py -H m0le.¬
it -p 22 -U users.txt -P ¬
dizionario.txt -T 2
[*] SSH Brute Force Ninja
[*] 1 user(s) loaded.
[*] 10 password(s) loaded.
[*] Brute Force started.
[*] Done.
```

Osserviamo quindi il comportamento dell'HIPS.
Come ci aspettavamo la generazione degli alert (via terminale, mail e WUI) ci informa puntualmente dell'accaduto:

```
** Alert 1269215496.1998: mail ¬
- syslog,sshd,authentication_ ¬
failures,
2010 Mar 22 17:13:30 www->/ ¬
var/log/authlog
Rule: 5720 (level 10) -> 'Mul
¬ tiple SSHD authentication ¬
failures.'
Src IP: 93.42.111.226
User: root
Mar 21 17:13:30 www sshd[3094]:¬
Failed password for root from ¬
93.42.111.226 port 26991 ssh2
Mar 21 17:13:29 www ¬
sshd[11785]: Failed password¬
for root from 93.42.111.226 ¬
port 35545 ssh2
```



*Un tipico esempio di avviso offerto dall'interfaccia web di OSSEC.*

Dopo poco, inoltre, la modalità A.R. si preoccupa di bloccare in modo definitivo l'IP che origina l'attacco aggiungendolo nel file hosts.deny e nella tabella ossec_fwtable di PF:

```
# tail -f /var/www/ossec/ ¬
logs/active-responses.log
Sun Mar 21 17:13:30 CET ¬
2010 .../host-deny.sh add ¬
93.42.111.226 1269188010. ¬
38989 5720
Sun Mar 21 17:13:30 CET ¬
2010 .../firewall-drop.sh add
¬ 93.42.111.226 1269188010. ¬
38989 5720

# pfctl -t ossec_fwtable -¬
T show
93.42.111.226

# cat /etc/hosts.deny
ALL:93.42.111.226
```

## 2 - WEB SERVER SCANNING

In questo caso utilizzeremo Nikto per analizzare il web server da remoto specificando come parametro di avvio l'abilitazione delle tecniche di IDS evasion:

```
# ./nikto.pl -evasion 1 -h ¬
m0le.it
...
```

Celermente il sistema di alerting ci notifica svariati errori riscontrati nel file di log degli accessi di Apache:

```
Rule: 31151 fired (level 10
¬) -> "Mutiple web server
400 ¬ error codes from same
¬ source ip."
Portion of the log(s):
93.42.111.226 - [22/ ¬
Mar/2010:01:06:15 +0100] ¬
"GET /fSf6Npjt.dat HTTP/ ¬
1.0" 404 206
93.42.111.226 - [22/ ¬
Mar/2010:01:27:14 +0100] ¬
"GET /fSf6Npjt/ HTTP/1.0" ¬
404 203
93.42.111.226 - [22/ ¬
Mar/2010:01:27:14 +0100] ¬
"GET /fSf6Npjt.UploadServlet
¬ HTTP/1.0" 404 216
...
```

Interessante constatare che, qualora avessimo Mod_Security abilitato, non mancherebbero avvisi relativi anche a quest'ultimo, come di seguito:

```
2010 Mar 22 01:06:02 www->/
¬ var/www/logs/error_log
Rule: 30118 (level 6) -> ¬
'Access attempt blocked by ¬
Mod Security.'
...
[Mon Mar 22 01:06:01 ¬
2010] [error] [client ¬
93.42.111.226] mod_security:
...
```

Dopo il chiasso fatto da Nikto, arriva puntuale come sempre la risposta del firewall:

```
#  tail -f /var/www/ossec/ ¬
logs/active-responses.log
Mon Mar 22 01:06:15 CET ¬
2010 .../host-deny.sh add -¬
93.42.111.226 1269216362. ¬
4217 30118
Mon Mar 22 01:06:16 CET
2010¬ .../firewall-drop.
sh add - ¬ 93.42.111.226
1269216362. ¬ 4217 30118
```

```
# pfctl -t ossec_fwtable ¬
-T show
93.42.111.226

# cat /etc/hosts.deny
ALL:93.42.111.226
```

## 3 - SEGFAULT SU MICROSOFT WINDOWS

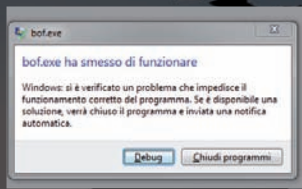
In questa circostanza osserveremo il comportamento di OSSEC quando un agente (in questo caso quello collocato sul PC montante Windows) invia informazioni relative a processi ed eventi dell'host entro cui è attivo. Simuleremo pertanto un crash di un generico applicativo suscettibile ai Buffer Overflow vedendo come l'HIPS intercetti l'apposito evento generato come Windows Event Log dal sistema immediatamente dopo il segfault.

Per far ciò utilizzeremo un banale sorgente che si commenta da solo (o almeno si spera), scritto per lo scopo:

```
#include <stdio.h>
main() {
char buf[3];
gets(buf);
return 0;
}
```

Compiliamo, avviamo ed inseriamo qualche carattere in più per constatare l'effettivo crash del "programma". Un'occhiata agli alert ci riconfermerà la meticolosità di OSSEC:

```
2010 Mar 22 01:40:11 (PC-¬
Windows1) 192.168.1.100-¬
>WinEvtLog
...
WinEvtLog: Application:
ERROR(1000): Application Er-
ror: (no user): no domain:
XXX: Nome dell'applicazio-
ne che ha generato l'erro-
re: bof.exe, ... timestamp:
0x4ba61368  Nome del modulo
che ha generato l'errore: ...
timestamp: 0x00000000  Codice
eccezione: 0xc0000005  Offset
errore 0x61616161
```




*L'inserimento di una stringa eccedente la dimensione del buffer causa, inevitabilmente, il crash del programma.*

## 4 - INTEGRITY CHECKING

Dal momento che Windows si presta bene ai nostri scopi esemplificativi, il nostro punto di riferimento sarà anche in questo caso l'agente "PC-Windows1".

Replicando il comportamento di un generico malware vedremo, operativamente, in cosa consiste il controllo di integrità condotto dall'HIPS, analizzando, come fatto finora, un alert generato.

La prima cosa che ci viene in mente di fare è modificare un file di sistema andandone a variare il checksum storicizzato da OSSEC in fase di primo avvio dell'agente.

Di seguito quindi l'immediato riscontro offerto dopo averne editato a mano uno a caso: "C:\Windows\win.ini":

```
Integrity checksum changed ¬
for: 'C:\Windows/win.ini'
Size changed from '403' to ¬
'409'
Old md5sum was: 'f3cb8893d927
¬ cb8edeee792928ecd1c9'
New md5sum is : '40f1bb10f0
¬ fc378289c3aaa722fb6d49'
Old sha1sum was: '24b0c156a97
¬ 4b4101304e51a6055d623-
b000a65d'
New sha1sum is : '24c15861a4
¬ e25e34013ffc7f38f8b2fbc8-
df6be8'
```

Il discorso è del tutto simile, ovviamente, per eventuali variazioni al registro di sistema.
Lasciamo al lettore le prove del caso.

## CONCLUSIONI E RIFERIMENTI

Appaiono evidenti le avanzate caratteristiche e peculiarità offerte dall'applicativo in qualunque contesto operativo; di gran lunga alla pari, se non migliori, rispetto alle alternative commerciali generalmente adoperate in contesti enterprise.

Risulterà quindi quasi scontato capire che, malgrado il discorso intrapreso sulla rivista sia stato pensato per offrire un quadro dell'HIDS quanto più esteso possibile, la quantità di azioni e processi gestibili da OSSEC è talmente notevole da rendere anche la nostra trattazione limitativa.

Come abbiamo avuto modo di segnalare, la documentazione è davvero tanta così come altrettanto grosse sono le possibilità offerte dalla suite. Anche qui, quindi, segnaliamo alcuni riferimenti, da intendersi come complementari a quelli già offerti nella prima parte di questo articolo.

Non ci resta che augurarvi buon divertimento e buona sperimentazione!

### RIFERIMENTI

Website relativi agli applicativi analizzati:

OpenBSD PF: www.openbsd.org/faq/pf/

Nikto: cirt.net/nikto2
Mod_Security: modsecurity.org

Alcune riferimenti online utili:

Buffer Overflow: www.siforge.org/articles/2003/04/15-bofexp.html

Buffer Overflow (2): www.owasp.org/index.php/Buffer_Overflow

Ulteriori riferimenti:
Hacker Journal nr. 195
"Buffer Overflow"



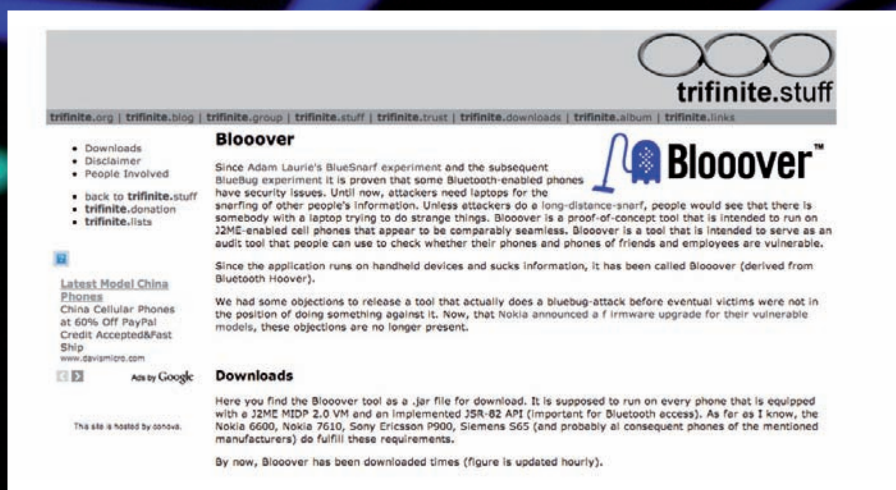
*Massimiano Rinaldi*
*redazione@hackerjournal.it*

# BLOOOVER: L'ASPIRATUTTO

MOBILE

## UN OTTIMO PROGRAMMA SCRITTO IN JAVA PER MONITORARE CELLULARI VULNERABILI VIA BLUETOOTH.

Vi piacerebbe collegarvi via bluetooth ad un cellulare "vittima" ed utilizzare la sua connettività per inviare sms, fare chiamate, tutto gratuitamente, oppure per impadronirvi della rubrica di quel telefono o di altri dati?
Potreste riuscirvi con Blooover (HYPERLINK "http://trifinite.org/trifinite_stuff_blooover.html" http://trifinite.org/trifinite_stuff_blooover.html) l'icona a forma di aspirapolvere rende un po' l'idea delle funzionalità insite in questo programma. Si tratta sostanzialmente di uno strumento di auditing per cellulari scritto in java (nella sezione download del sito potete scaricare tutte le versioni che pesano pochi KB).
Il fatto di essere stato scritto nativamente in Java consente a Blooover di essere, in linea teorica, multipiattaforma, ovvero supportato da tutti i telefoni java con MIDP2 (mobile Information Device Profile).




### LE FUNZIONI

Questo programma nasce con l'intento di rivelare telefoni vulnerabili, quindi come strumento di monitoraggio, ma, chiaramente può essere reverse-engineered per scopi meno edificanti.
Sembrerebbe tutto bellissimo però tutto sommato Blooover ha una capacità di attacco limitata, in effetti i modelli attaccabili con successo sono pochi, quelli dichiarati sono piuttosto datati si tratta di:
Nokia 6600, Nokia 7610, Sony Ericsson P900 e Siemens S65.
E' evidente come tutti questi telefoni risalgano grosso modo agli anni 2005/2006 ovvero il periodo in cui è stato rilasciato il programma che poi, a dire il vero, è stato aggiornato poco.
Comunque per non farci mancare nulla abbiamo fatto una prova installando la versione bredder (che trovate naturalmente sul sito) su un recente Nokia N95 che abbiamo utilizzato come attaccante.
La vittima designata è stata identificata in un vecchio Nokia 660 che è tornato buono per l'utilizzo.

### LA PROVA

Dopo avere inviato via bluetooth il file .jar dal computer al Nokia N95 e avere installato il programma, abbiamo lanciato Blooover.

La schermata iniziale propone una serie di opzioni:

Find Devices
Settings
Reports



Breed Blooover2
About Blooover II
Exiet Blower II
Scegliendo Find Devices o Breed Blooover2 il programma inizia la scansione dei terminali con la porta bluetooth attivata. Nel nostro caso ha rilevato il Nokia 6600, ma anche il computer.
Una volta evidenziato il nome del cellulare “vittima” sul display del cellulare “attaccante” nel nostro caso il Nokia N95, vengono proposti una serie di attacchi:

## HELOMOTO

I cellulari vulnerabili accettano un altro cellulare che tenta un trasferimento OBEX PUSH. Questo consente una connessione al profilo Headset del cellulare che permette un accesso non protetto all’AT Command PArser. Questa falla è stata scoperta nel “lontano” maggio 2005 da Adam Laurie.

## BLUESNARF

E’ impostato sul profilo OBEX Push. Si connette alla maggior parte dei servizi OPP e richiede nomi di file conosciuti dalle specifiche Irmc invece di inviare un file .vcf.
La sua scoperta risale al 2003.

## BLUESNARF++

E’, come suggerisce il nome, assai simile a Bluesnarf. La differenza è che nel Bluesnarf ++ l’hacker può leggere o scrivere liberamente nel filesystem.
Bluesnarf ++ dà pieno accesso per scrivere o leggere quando ci si connette all’OBEX Push profile. Il filesystem include infine espansioni di memoria come memory sticks o SD card.

## BLUEBUG

Si basa sull’At command parser che viene fornito come un servizio nascosto utilizzato esclusivamente per gli auricolari. Bluebug permette di leggere e scrivere i contatti della rubrica, leggere e inviare sms e chiamare un numero con il cellulare “attaccato”. Questo attacco è stato scoperto da Martin Herfurt nel febbraio 2004,

## MALFORMED OBJECTS

Con questo tipo di attacco, particolarmente dannoso, i cellulari vulnerabili si spengono quando ricevono per esempio un biglietto da visita malformato.
Questo porta all’instabilità del parser del cellulare e spesso porta a comportamenti imprevedibili (incluso il crash del cellulare).

Gli attacchi attivi presentano un segno di spunta. Non vi resta che selezionare il tipo di attacco partendo magari da BlueBug e scegliere Select. Blooover inizierà a lavorare sul cellulare vittima.
Nel nostro caso abbiamo optato per le impostazioni di default con un attacco combinato Helo moto, Bluebug e Bluesnarf. Blooover in fase di scansione ci ha chiesto se volevamo utilizzare la connettività del cellulare vittima (perfetto) però sul Nokia 6600 è stato visualizzato un messaggio in cui si invitava l’utente ad accettare un messaggio bluetooth da un altro cellulare. Insomma, ci vuole un po’ di collaborazione…
Dando l’ok in effetti Blooover ha dato accesso alla rubrica e ha consentito l’invio di SMS, a sbafo, con Bluebug. E’ consigliabile utilizzare un attacco per volta perché, ad esempio, se il cellulare vittima non è dotato di connettività Blooover si chiude senza eseguire altri attacchi combinati. Si tratta naturalmente di una prova circoscritta. Però il programma è a disposizione per fare esperimenti di vario tipo, magari fateci sapere le vostre esperienze, siamo curiosi…

